Avira Internet Security

Benutzerhandbuch





Warenzeichen und Copyright

Warenzeichen

Windows ist ein registriertes Warenzeichen der Microsoft Corporation in den Vereinigten Staaten und anderen Ländern.
Alle anderen Marken- und Produktnamen sind Warenzeichen oder eingetragene Warenzeichen ihrer entsprechenden Besitzer.
Geschützte Warenzeichen sind in diesem Handbuch nicht als solche gekennzeichnet. Dies bedeutet jedoch nicht, dass sie frei verwendet werden dürfen.

Hinweise zum Copyright

Für Avira Internet Security wird Code von Drittanbietern verwendet. Wir bedanken uns bei den Copyright-Inhabern dafür, dass sie uns ihren Code zur Verfügung gestellt haben.
Detaillierte Informationen zum Copyright finden Sie in der Programmhilfe von Avira Internet Security unter "Third Party Licenses".



Inhaltsverzeichnis





1. Einleitung

Mit Ihrem Avira Produkt schützen Sie Ihren Computer vor Viren, Würmern, Trojanern, Ad- und Spyware sowie weiteren Gefahren. Verkürzend wird in diesem Handbuch von Viren oder Malware (Schadsoftware) und unerwünschten Programmen gesprochen.

Das Handbuch beschreibt die Installation und Bedienung des Programms.

Auf unserer Webseite können Sie vielfältige Optionen und weitere Informationsmöglichkeiten nutzen:

http://www.avira.de

Sie können auf der Avira Webseite:

- Informationen zu weiteren Avira Desktop-Programmen abrufen
- die aktuellsten Avira Desktop-Programme herunterladen
- die aktuellsten Produkthandbücher im Format PDF herunterladen
- kostenfreie Support- und Reparatur-Werkzeuge herunterladen
- die umfassenden Wissensdatenbank und FAQ-Artikel bei der Behebung von Problemen nutzen
- die landesspezifischen Supportadressen abrufen.

Ihr Avira Team

1.1 Symbole und Hervorhebungen

Folgende Symbole werden verwendet:

Symbol / Bezeichnung	Erläuterung
✓	Steht vor einer Voraussetzung, die vor dem Ausführen einer Handlung erfüllt sein muss.
▸	Steht vor einem Handlungsschritt, den Sie ausführen.
↳	Steht vor einem Ergebnis, das aus der vorangehenden Handlung folgt.
Warnung	Steht vor einer Warnung bei Gefahr von kritischem Datenverlust.



Hinweis	Steht vor einem Hinweis mit besonders wichtigen Informationen oder vor einem Tipp, der das Verständnis und die Nutzung Ihres Avira Produkts erleichtert.

Folgende Hervorhebungen werden verwendet:

Hervorhebung	Erläuterung
Kursiv	Dateiname oder Pfadangabe.
	Elemente der Software-Oberfläche, die angezeigt werden (z.B. Fensterbereich oder Fehlermeldung).
Fett	Elemente der Software-Oberfläche, die angeklickt werden (z.B. Menüpunkt, Rubrik, Optionsfeld oder Schaltfläche).

2. Produktinformationen

In diesem Kapitel erhalten Sie alle Informationen, die für den Erwerb und Einsatz Ihres Avira Produkts relevant sind:

- siehe Kapitel: Leistungsumfang
- siehe Kapitel: Systemvoraussetzungen
- siehe Kapitel: Lizenzierung und Upgrade
- siehe Kapitel: Lizenzverwaltung

Avira Produkte bieten umfassende und flexible Werkzeuge, um Ihren Computer zuverlässig vor Viren, Malware, unerwünschten Programmen und sonstigen Gefahren zu schützen.

- Beachten Sie:

Warnung
Der Verlust wertvoller Daten hat meist dramatische Folgen. Auch das beste Virenschutzprogramm kann Sie nicht hundertprozentig vor Datenverlust schützen. Fertigen Sie regelmäßig Sicherungskopien (Backups) Ihrer Daten an.

Hinweis
Ein Programm, das vor Viren, Malware, unerwünschten Programmen und sonstigen Gefahren schützt, ist nur dann zuverlässig und wirksam, wenn es aktuell ist. Stellen Sie die Aktualität Ihres Avira Produkts über automatische Updates sicher. Konfigurieren Sie das Programm entsprechend.

2.1 Leistungsumfang

Ihr Avira Produkt verfügt über folgende Funktionen:

- Control Center zur Überwachung, Administration und Steuerung des gesamten Programms
- Zentrale Konfiguration mit benutzerfreundlicher Standard- und Expertenkonfiguration und kontextsensitiver Hilfe
- System-Scanner (On-Demand Scan) mit profilgesteuerter und konfigurierbarer Suche nach allen bekannten Typen von Viren und Malware
- Integration in die Windows Benutzerkontensteuerung (User Account Control), um Aufgaben durchführen zu können, für die administrative Rechte erforderlich sind.
- Echtzeit-Scanner (On-Access Scan) zur ständigen Überwachung sämtlicher Dateizugriffe

- ProActiv-Komponente zur permanenten Überwachung von Programmaktionen (nur für 32-Bit-Systeme)
- Email-Schutz (POP3-Scanner, IMAP-Scanner und SMTP-Scanner) zur permanenten Kontrolle Ihrer Emails auf Viren und Malware, inklusive Überprüfung der Email-Anhänge
- Avira SearchFree Toolbar, eine im Webbrowser integrierte Suchleiste, mit der Sie schnell und bequem das Internet durchsuchen können. Sie beinhaltet auch Widgets zu den wichtigsten Funktionen rund ums Internet.
- Browser-Schutz zur Überwachung der aus dem Internet per HTTP-Protokoll übertragenen Daten und Dateien (Überwachung der Ports 80, 8080, 3128)
- Avira Kinderschutz für Soziale Netzwerke informiert Eltern über die Onlineaktivitäten ihrer Kinder. Die Konten bei sozialen Netzwerken werden auf Kommentare, Fotos etc. überprüft, die dem Ruf Ihres Kindes schaden könnten oder die darauf hinweisen könnten, dass sich Ihr Kind in Gefahr befindet.
- Kinderschutz-Komponente zum rollenbasierten Filtern von unerwünschten Webseiten und zur zeitlichen Beschränkung der Internetnutzung
- Avira Free Android Security ist eine App zum Schutz vor Diebstahl und/oder Verlust. Die App bietet Funktionen, mit deren Hilfe Sie das mobile Gerät ausfindig machen können, wenn Sie es verlegt haben oder schlimmer noch: wenn es gestohlen wurde. Des Weiteren ermöglicht Ihnen die App, eingehende Anrufe und SMS zu blockieren. Avira Free Android Security schützt Mobiltelefone und Smartphones, die mit dem Betriebssystem Android arbeiten.
- Backup-Komponente zur Erstellung von Backups Ihrer Daten (Spiegel-Backups)
- Integriertes Quarantäne-Management zur Isolation und Behandlung verdächtiger Dateien
- Rootkits-Schutz zum Auffinden von Malware, die versteckt im System des Rechners installiert wurde (sog. Rootkits) (nicht verfügbar unter Windows XP 64 Bit)
- Direkter Zugriff auf detaillierte Informationen zu gefundenen Viren und Malware über das Internet
- Einfaches und schnelles Update des Programms, der Virendefinitionsdateien (VDF) sowie der Suchengine durch Single File Update und inkrementelles VDF-Update über einen Webserver im Internet
- Benutzerfreundliche Lizenzierung in der Lizenzverwaltung
- Integrierter Planer zur Festsetzung von einmaligen oder wiederkehrenden Aufgaben wie Updates oder Prüfläufen
- Extrem hohe Viren- und Malware-Erkennung durch innovative Suchtechnologien (Suchengine) inklusive heuristischer Suchverfahren
- Erkennung aller gebräuchlichen Archivtypen inklusive Erkennung verschachtelter Archive und Smart-Extension-Erkennung
- Hohe Performanz durch Multithreading-Fähigkeit (gleichzeitiges Scannen vieler Dateien mit hoher Geschwindigkeit)

- FireWall zum Schutz Ihres Computers vor unerlaubten Zugriffen aus dem Internet bzw. aus einem Netzwerk sowie vor unerlaubten Zugriffen auf das Internet/Netzwerk durch nicht autorisierte Benutzer

2.2 Systemvoraussetzungen

2.2.1 Systemvoraussetzungen

Avira Internet Security stellt für einen erfolgreichen Einsatz folgende Anforderungen an das System:

Betriebssystem

- Windows XP, neuestes SP (32 oder 64 Bit) oder
- Windows 7, neuestes SP (32 oder 64 Bit)

> **Hinweis**
> Die Windows 8-Zertifizierung für Avira Internet Security ist in Bearbeitung.

Hardware

- Computer ab Pentium, mindestens 1 GHz
- Mindestens 150 MB freier Speicherplatz auf der Festplatte (bei Verwendung der Quarantäne und für temporären Speicher mehr)
- Mindestens 512 MB Arbeitsspeicher unter Windows XP
- Mindestens 1024 MB Arbeitsspeicher unter Windows 7

Weitere Voraussetzungen

- Für die Programminstallation: Administrator-Rechte
- Für alle Installationen: Windows Internet Explorer 6.0 oder höher
- Ggf. Internetverbindung (siehe Installation)

2.2.2 Avira SearchFree Toolbar

Folgende Voraussetzungen sind eine reibungslose Nutzung der Avira SearchFree Toolbar erforderlich:

Betriebssystem

- Windows XP, neuestes SP (32 oder 64 Bit) oder
- Windows 7, neuestes SP (32 oder 64 Bit)

Webbrowser

- Windows Internet Explorer 6.0 oder höher
- Mozilla Firefox 3.0 oder höher

- Google Chrome 18.0 oder höher

> **Hinweis**
> Bitte deinstallieren Sie ggf. bereits installierte Suchleisten vor der Installation der Avira SearchFree Toolbar. Anderenfalls ist eine Installation der Avira SearchFree Toolbar nicht möglich.

2.2.3 Hinweise für die Benutzer von Windows Vista oder höher

Unter Windows XP arbeiten viele Benutzer mit Administratorrechten. Dies ist unter Sicherheitsaspekten jedoch nicht wünschenswert, denn so haben auch Viren und unerwünschte Programme leichtes Spiel, sich im Computer einzunisten.

Aus diesem Grund führte Microsoft die "Benutzerkontensteuerung" (User Account Control) ein. Diese ist Teil folgender Betriebssysteme:

- Windows Vista
- Windows 7
- Windows 8

Die Benutzerkontensteuerung bietet mehr Schutz für Anwender, die als Administrator angemeldet sind. So verfügt ein Administrator zunächst nur über die Privilegien eines normalen Benutzers. Aktionen, für die Administratorrechte erforderlich sind, markiert das Betriebssystem klar mit einem Hinweis-Icon. Zudem muss der Anwender die gewünschte Aktion explizit bestätigen. Erst, nachdem diese Zustimmung eingeholt ist, findet eine Erhöhung der Privilegien statt, und das Betriebssystem führt die jeweilige administrative Aufgabe aus.

Das Avira Produkt benötigt für einige Aktionen Administratorrechte. Diese Aktionen werden mit folgendem Zeichen gekennzeichnet: . Erscheint dieses Zeichen zusätzlich auf einer Schaltfläche, so werden zum Ausführen dieser Aktion Administratorrechte benötigt. Besitzt Ihr aktuelles Benutzerkonto keine Administratorrechte, so fordert Sie der Windows-Dialog zur Benutzerkontensteuerung zur Eingabe des Administratorkennworts auf. Verfügen Sie über kein Administratorkennwort, so können Sie diese Aktion nicht ausführen.

2.3 Lizenzierung und Upgrade

2.3.1 Lizenzierung

Um Ihr Avira Produkt nutzen zu können, benötigen Sie eine Lizenz. Sie erkennen damit die Lizenzbedingungen an.

Die Lizenz wird in Form eines Aktivierungscodes vergeben. Der Aktivierungscode ist ein Buchstaben-Zahlen-Code, den Sie beim Erwerb des Avira Produkts erhalten. Über den

Aktivierungscode sind die genauen Daten Ihrer Lizenz, d.h. welche Programme für welchen Zeitraum lizenziert wurden, erfasst.

Der Aktivierungscode wird Ihnen in einer Email übermittelt, falls Sie Ihr Avira Produkt im Internet erworben haben, oder ist auf der Produktverpackung vermerkt.

Um Ihr Programm zu lizenzieren, geben Sie den Aktivierungscode bei der Aktivierung des Programms ein. Die Produktaktivierung kann bei der Installation erfolgen. Sie können Ihr Avira Produkt jedoch auch nach der Installation im Lizenzmanager unter **Hilfe > Lizenzmanagement** aktivieren.

2.3.2 Lizenzverlängerung

Wenn Ihre Lizenz in Kürze abläuft, erinnert Sie Avira durch ein Slide-Up, sie zu verlängern. Um dies zu tun, müssen Sie nur einen Link klicken und Sie werden zum Avira Online-Shop weitergeleitet. Es ist aber auch möglich, die Lizenz Ihres Avira Produkts durch den Lizenzmanager zu verlängern, unter **Hilfe > Lizenzmanagement**.

Wenn Sie sich im Lizenzportal von Avira registriert haben, können Sie Ihre Lizenz auch zusätzlich durch die **Lizenzübersicht** verlängern oder die automatische Verlängerung wählen.

2.3.3 Upgrade

Im Lizenzmanager haben Sie die Möglichkeit, ein Upgrade auf ein Produkt aus der Avira Desktop-Produktfamilie anzustoßen: Eine manuelle Deinstallation des alten Produkts und eine manuelle Installation des neuen Produkts sind dadurch nicht erforderlich. Beim Upgrade aus dem Lizenzmanager geben Sie den Aktivierungscode des Produkts, auf das Sie umsteigen möchten, im Eingabefeld des Lizenzmanagers an. Es erfolgt eine automatische Installation des neuen Produkts.

Um hohe Zuverlässigkeit und Sicherheit für Ihren Computer zu erreichen, erinnert Sie Avira an das anstehende Upgrade auf die neueste Version. Klicken Sie auf **Upgrade** in dem Popup-Element, um auf die produktspezifische Upgrade-Seite Ihres Produkts weitergeleitet zu werden. Sie haben die Möglichkeit, für Ihr derzeitiges Produkt ein Upgrade durchzuführen oder ein umfangreicheres Avira Produkt zu erwerben. Die Übersichtsseite der Avira Produkte zeigt Ihnen, welches Produkt Sie gegenwärtig verwenden und gibt Ihnen die Möglichkeit, dieses mit anderen Avira Produkten zu vergleichen. Für weitere Informationen klicken Sie das Informations-Symbol rechts neben dem Produktnamen an. Wenn Sie bei Ihrem bisherigen Produkt bleiben möchten, klicken Sie **Upgrade**, um sofort die neueste Version mit verbesserten Funktionen zu installieren. Wenn Sie ein umfangreicheres Produkt erwerben möchten, klicken Sie **Kaufen** am unteren Ende der entsprechenden Produktspalte. Sie werden dann in den Avira Online-Shop weitergeleitet, um Ihre Bestellung durchzuführen.

Hinweis
In Abhängigkeit von Ihrem Produkt und Ihrem Betriebssystem benötigen Sie eventuell Administratorrechte, um das Upgrade durchzuführen. Melden Sie sich als Administrator an, bevor Sie ein Upgrade ausführen.

2.3.4 Lizenzverwaltung

Die Avira Internet Security Lizenzverwaltung ermöglicht eine sehr einfache Installation der Avira Internet Security Lizenz.

Avira Internet Security Lizenzverwaltung



Sie können eine Installation der Lizenz vornehmen, in dem Sie in ihrem Dateimanager oder der Aktivierungs-Email mit Doppelklick die Lizenzdatei auswählen und den entsprechenden Bildschirmanweisungen folgen.

Hinweis
Die Avira Internet Security Lizenzverwaltung kopiert die entsprechende Lizenz automatisch in den entsprechenden Produktordner. Ist bereits eine Lizenz vorhanden, erscheint ein Hinweis, ob die bestehende Lizenzdatei ersetzt



werden soll. Die bereits bestehende Datei wird in diesem Fall mit der aktuellen Lizenzdatei überschrieben.

3. Installation und Deinstallation

In diesem Kapitel erhalten Sie Informationen rund um die Installation und Deinstallation Ihres Avira Produkts:

- siehe Kapitel: Installationsarten: Unterschiede zwischen Express- und benutzerdefinierter Installtion
- siehe Kapitel: Vor der Installation: Voraussetzungen, Vorbereitung des Computers auf die Installation
- siehe Kapitel: Expressinstallation: Standardinstallation gemäß der Voreinstellungen
- siehe Kapitel: Benutzerdefinierte Installation: Konfigurierbare Installation
- siehe Kapitel: Testprodukt Installation
- siehe Kapitel: Konfigurationsassistent
- siehe Kapitel: Änderungsinstallation
- siehe Kapitel: Installationsmodule
- siehe Kapitel: Deinstallation: Deinstallation durchführen

3.1 Installationsarten

Während der Installation können Sie im Installationsassistenten einen Setup-Typ wählen:

Express

- Die Standardkomponenten werden installiert.
- Die Programmdateien werden in ein vorgegebenes Standardverzeichnis unter *C:\Programme* installiert.
- Ihr Avira Produkt wird mit Standardeinstellungen installiert. Sie haben keine Möglichkeit, Voreinstellungen im Konfigurationsassistenten vorzunehmen.

Benutzerdefiniert

- Sie haben die Möglichkeit, einzelne Programmkomponenten zur Installation auszuwählen (siehe Kapitel Installation und Deinstallation > Installationsmodule).
- Es kann ein Zielordner für die zu installierenden Programmdateien gewählt werden.
- Sie können festlegen, ob eine Verknüpfung auf Ihrem Desktop und/oder eine Programmgruppe im Startmenü erstellt werden soll.
- Mithilfe des Konfigurationsassistenten können Sie benutzerdefinierte Einstellungen für Ihr Avira Produkt vornehmen und eine kurze Systemprüfung direkt nach der Installation veranlassen.

3.2 Vor der Installation

> **Hinweis**
> Überprüfen Sie vor der Installation, ob Ihr Computer die Systemvoraussetzungen erfüllt. Falls Ihr Computer alle Voraussetzungen erfüllt, können Sie das Avira Produkt installieren.

Initialisierung vor der Installation

✓ Schließen Sie Ihr Email-Programm. Es wird außerdem empfohlen, alle laufenden Anwendungen zu beenden.

✓ Vergewissern Sie sich, dass keine weiteren Virenschutzlösungen installiert sind. Die automatischen Schutzfunktionen verschiedener Sicherheitslösungen können sich gegenseitig behindern.

- ↪ Das Avira Produkt wird Ihren Computer auf mögliche inkompatible Software durchsuchen.
- ↪ Bei Fund inkompatibler Software wird eine entsprechende Liste dieser Programme generiert.
- ↪ Es wird empfohlen Software, die die Sicherheit Ihres Computers gefährdet, zu deinstallieren.

▶ Wählen Sie aus der Liste jene Programme, die automatisch von Ihrem Computer entfernt werden sollen und klicken Sie **Weiter**.

▶ Einige Programme lassen sich nur manuell von Ihrem Computer entfernen. Wählen Sie die Programme aus und klicken Sie **Weiter**.

- ↪ Die Deinstallation eines oder mehrerer Programme erfordert den Neustart Ihres Computers. Nach dem Neustart wird die Installation fortgeführt.

> **Warnung**
> Ihr Computer ist ungeschützt bis der Installationsvorgang des Avira Produktes abgeschlossen ist.

Installation

Das Installationsprogramm funktioniert im selbsterklärenden Dialogmodus. Bei der Mehrzahl der Installationsschritte ist ein einfacher Klick ausreichend, um fortzufahren.

Die wichtigsten Schaltflächen sind mit folgenden Funktionen belegt:

- **OK**: Aktion bestätigen.
- **Abbrechen**: Aktion abbrechen.
- **Weiter**: Zum nächsten Schritt übergehen.

- **Zurück**: Zum vorangegangenen Schritt zurückgehen.

▸ Stellen Sie eine Internetverbindung her. Die Internetverbindung wird zur Ausführung folgender Installationsschritte benötigt:

- Herunterladen der aktuellen Programmdateien und der Suchengine sowie der tagesaktuellen Virendefinitionsdateien durch das Installationsprogramm (bei internetbasierter Installation)
- Aktivierung des Programms
- Ggf. Ausführung eines Updates nach beendeter Installation

▸ Halten Sie den Aktivierungscode oder die Lizenzdatei für Ihr Avira Produkt bereit, wenn Sie das Programm aktivieren möchten.

Hinweis
Internetbasierte Installation:
Zur internetbasierten Installation des Programms steht ein Installationsprogramm zur Verfügung, welches die aktuellen Programmdateien vor der Ausführung der Installation von den Avira Webservern lädt. Durch dieses Verfahren wird gewährleistet, dass Ihr Avira Produkt mit einer tagesaktuellen Virendefinitionsdatei installiert wird.

Installation mit einem Installationspaket:
Das Installationspaket enthält sowohl das Installationsprogramm als auch alle benötigten Programmdateien. Es besteht bei der Installation mit einem Installationspaket jedoch keine Sprachauswahl für Ihr Avira Produkt. Es wird empfohlen im Anschluss an die Installation, ein Update auszuführen, um die Virendefinitionsdatei zu aktualisieren.

Hinweis
Zur Produktaktivierung kommuniziert Ihr Avira Produkt über das HTTP-Protokoll und Port 80 (Web-Kommunikation) sowie über das Verschlüsselungsprotokoll SSL und Port 443 mit den Avira Servern. Falls Sie eine Firewall nutzen, stellen Sie sicher, dass die benötigten Verbindungen und eingehende oder ausgehende Daten nicht von der Firewall blockiert werden.

3.3 Expressinstallation

So installieren Sie Ihr Avira Produkt:

Starten Sie das Installationsprogramm mit einem Doppelklick auf die Installationsdatei, die Sie aus dem Internet heruntergeladen haben, oder legen Sie die Programm-CD ein.

Internetbasierte Installation

↳ Das Dialogfenster **Willkommen** erscheint.



- Klicken Sie auf **Weiter**, um mit der Installation fortzufahren.
  - ↳ Das Dialogfenster **Sprachauswahl** erscheint.
- Wählen Sie die Sprache aus, in der Sie Ihr Avira Produkt installieren möchten und bestätigen Sie Ihre Sprachauswahl mit **Weiter**.
  - ↳ Das Dialogfenster **Download** erscheint. Alle zur Installation benötigten Dateien werden von den Avira Webservern heruntergeladen. Nach Abschluss des Downloads schließt sich das Fenster **Download**.

Installation mit einem Installationspaket

- ↳ Das Fenster **Installation wird vorbereitet** erscheint.
- ↳ Die Installationsdatei wird entpackt. Die Installationsroutine wird gestartet.
- ↳ Das Dialogfenster **Installationsart wählen** erscheint.

> **Hinweis**
> Standardmäßig ist die **Expressinstallation**, bei der die Standardkomponenten ohne Konfigurationsmöglichkeiten installiert werden, voreingestellt. Möchten Sie eine **Benutzerdefinierte Installation** durchführen, lesen Sie bitte hier weiter: Installation und Deinstallation > Benutzerdefinierte Installation.

- Die Option **Ich möchte meinen Schutz mit Avira ProActiv und Cloud-Sicherheit verbessern** ist voreingestellt (Konfiguration > Allgemeines > Erweiterter Schutz). Sie haben die Möglichkeit, an der Avira Community nicht teilzunehmen, indem Sie das Kontrollkästchen deaktivieren.
  - ↳ Avira sendet Daten zu verdächtigen Programmen an das Avira Malware Research Center. Die Daten werden allein zu einer erweiterten Onlineprüfung und zur Erweiterung und Verfeinerung der Erkennungstechnologie genutzt. Über die Links **ProActiv** und **Cloud-Sicherheit** können Sie Details zur erweiterten Online-Prüfung abrufen.
- Bestätigen Sie, dass Sie die **Endbenutzer-Lizenzvereinbarung** akzeptieren. Wenn Sie die Details der Lizenzvereinbarung lesen möchten, klicken Sie auf den entsprechenden Link.
- Klicken Sie **Weiter**.
  - ↳ Der *Lizenz-Assistent* wird geöffnet und unterstützt Sie bei der Aktivierung Ihres Programms.
  - ↳ An dieser Stelle haben Sie die Möglichkeit, einen Proxy Server zu konfigurieren.
- Klicken Sie ggf. **Proxy Einstellungen**, um den Proxy Server zu konfigurieren und bestätigen Sie Ihre Einstellungen mit **OK**.
- Wenn Sie bereits einen Aktivierungscode erhalten haben, wählen Sie **Produkt aktivieren** aus und geben Sie anschließend Ihren Code ein.

  -ODER-

- Wenn Sie noch keinen Aktivierungscode haben, klicken Sie den Link **erwerben Sie einen Aktivierungscode**.
  - ↳ Sie werden zur Avira Webseite weitergeleitet.

  Alternativ klicken Sie auf den Link **Ich habe bereits eine gültige Lizenzdatei**.
- Markieren Sie im Dialog **Datei Öffnen** die *.KEY*-Datei und klicken Sie **Öffnen**.
  - ↳ Der Aktivierungscode wird in den Lizenz-Assistenten kopiert.
- Möchten Sie das Produkt testen, lesen Sie bitte im Kapitel Testprodukt Installation weiter.
- Klicken Sie **Weiter**.
  - ↳ Der Installationsfortschritt wird durch einen grünen Balken dargestellt.
  - ↳ Das Dialogfenster **Schließen Sie sich Millionen von Avira-Nutzern an, die bereits Avira SearchFree nutzen** erscheint.
- Wenn Sie die Avira SearchFree Toolbar nicht installieren möchten, entfernen Sie die Markierung aus dem Kästchen der Avira SearchFree Toolbar und Avira SearchFree Updater **Lizenzvereinbarung** und deaktivieren Sie die Festlegung von **Avira SearchFree (search.avira.com)** als Startseite.

> **Hinweis**
> Bitte deinstallieren Sie ggf. bereits installierte Suchleisten vor der Installation der Avira SearchFree Toolbar. Anderenfalls ist eine Installation der Avira SearchFree Toolbar nicht möglich.

- Klicken Sie **Weiter**.
  - ↳ Der Installationsfortschritt der Avira SearchFree Toolbar wird durch einen grünen Balken dargestellt.
  - ↳ Das Avira Tray Icon ist in der Taskleiste platziert.
  - ↳ Das Modul **Updater** sucht nach möglichen Aktualisierungen, um Ihren Computer optimal zu schützen.
  - ↳ Das Statusfenster **Luke Filewalker** öffnet sich zu einer ersten Scanner-Direktsuche, informiert Sie über den Stand der Prüfung und zeigt die Ergebnisse an.
- Falls Sie nach der Systemprüfung zu einem Systemneustart aufgefordert werden sollten, führen Sie diesen durch, damit Ihr System vollständig geschützt ist.

  Nach der erfolgreichen Installation wird empfohlen, im Bereich **Status** im Control Center die Aktualität des Schutzprogramms zu prüfen.
- Zeigt Ihr Avira Produkt, dass Ihr Computer nicht vollständig geschützt ist, klicken Sie **Problem beheben**.
  - ↳ Das Dialogfenster **Schutz wiederherstellen** öffnet sich.

- Maximieren Sie die Sicherheit Ihres Systems, indem Sie die vorgegebenen Optionen aktivieren.
- Führen Sie ggf. im Anschluss eine vollständige Systemprüfung durch.

3.4 Benutzerdefinierte Installation

So installieren Sie Ihr Avira Produkt:

Starten Sie das Installationsprogramm mit einem Doppelklick auf die Installationsdatei, die Sie aus dem Internet heruntergeladen haben, oder legen Sie die Programm-CD ein.

Internetbasierte Installation

↳ Das Dialogfenster **Willkommen** erscheint.

- Klicken Sie auf **Weiter**, um mit der Installation fortzufahren.

↳ Das Dialogfenster **Sprachauswahl** erscheint.

- Wählen Sie die Sprache aus, in der Sie Ihr Avira Produkt installieren möchten und bestätigen Sie Ihre Sprachauswahl mit **Weiter**.

↳ Das Dialogfenster **Download** erscheint. Alle zur Installation benötigten Dateien werden von den Avira Webservern heruntergeladen. Nach Abschluss des Downloads schließt sich das Fenster **Download**.

Installation mit einem Installationspaket

↳ Das Fenster **Installation wird vorbereitet** erscheint.

↳ Die Installationsdatei wird entpackt. Die Installationsroutine wird gestartet.

↳ Das Dialogfenster **Installationsart wählen** erscheint.

Hinweis
Standardmäßig ist die **Expressinstallation**, bei der die Standardkomponenten ohne Konfigurationsmöglichkeiten installiert werden, voreingestellt. Möchten Sie diese durchführen, lesen Sie bitte hier weiter: Installation und Deinstallation > Expressinstallation.

- Wählen Sie **Benutzerdefiniert** als die gewünschte Installationsart aus.
- Die Option **Ich möchte meinen Schutz mit Avira ProActiv und Cloud-Sicherheit verbessern** ist voreingestellt. Sie haben die Möglichkeit, an der Avira Community nicht teilzunehmen, indem Sie das Kontrollkästchen deaktivieren.

↳ Avira sendet Daten zu verdächtigen Programmen an das Avira Malware Research Center. Die Daten werden allein zu einer erweiterten Onlineprüfung und zur Erweiterung und Verfeinerung der Erkennungstechnologie genutzt. Über die Links **ProActiv** und **Cloud-Sicherheit** können Sie Details zur erweiterten Online-Prüfung abrufen.



- Bestätigen Sie, dass Sie die **Endbenutzer-Lizenzvereinbarung** akzeptieren. Wenn Sie die Details der Lizenzvereinbarung lesen möchten, klicken Sie auf den entsprechenden Link.
- Klicken Sie **Weiter**.
  - ↳ Das Fenster **Zielverzeichnis wählen** öffnet sich.
  - ↳ Voreingestellt ist das Verzeichnis *C:\Programme\Avira\AntiVir Desktop*
- Klicken Sie **Weiter**, um mit der Installation fortzufahren.

- ODER -

- Wählen Sie mit **Durchsuchen** ein anderes Zielverzeichnis und bestätigen Sie mit **Weiter**.
  - ↳ Das Dialogfenster **Komponenten installieren** erscheint.
- Aktivieren oder deaktivieren Sie die gewünschten Komponenten und bestätigen Sie mit **Weiter**.
- Wenn Sie die **Cloud-Sicherheit**-Komponente ausgewählt haben, Sie jedoch jedesmal manuell bestätigen möchten, welche Dateien zur Cloud-Analyse hochgeladen werden sollen, aktivieren Sie die Option **Manuell bestätigen, wenn verdächtige Dateien an Avira Operations GmbH & Co. KG gesendet werden**.
- Klicken Sie **Weiter**.
- Im folgenden Dialogfenster können Sie festlegen, ob eine Verknüpfung auf Ihrem Desktop und/oder eine Programmgruppe im Startmenü erstellt werden soll.
- Klicken Sie **Weiter**.
  - ↳ Der **Lizenz-Assistent** wird geöffnet.

Sie haben folgende Optionen zur Aktivierung des Programms zur Auswahl:

- Eingabe eines Aktivierungscodes
  - ↳ Durch die Eingabe Ihres Aktivierungscodes wird Ihr Avira Produkt mit Ihrer Lizenz aktiviert.
- Kauf eines Aktivierungscodes
  - ↳ Wenn Sie den Link **erwerben Sie einen Aktivierungscode** klicken, werden Sie zur Avira Webseite weitergeleitet.
- Auswahl der Option **Produkt testen**
  - ↳ Wählen Sie **Produkt testen**, wird beim Aktivierungsvorgang eine Testlizenz generiert, mit der das Programm aktiviert wird. Sie können das Avira Produkt für einen bestimmten Zeitraum in seinem vollen Funktionsumfang testen (siehe Testprodukt Installation).

> **Hinweis**
> Mit der Option **Ich habe bereits eine gültige Lizenzdatei** können Sie eine

gültige Lizenzdatei einlesen. Die Lizenzdatei wird beim Vorgang der Produktaktivierung mit einem gültigen Aktivierungscode generiert und im Programmverzeichnis Ihres Avira Produkts abgelegt. Nutzen Sie diese Option, wenn Sie eine Produktaktivierung bereits durchgeführt haben und Ihr Avira Produkt neu installieren möchten.

Hinweis
Bei einigen Verkaufsversionen von Avira Produkten ist ein Aktivierungscode bereits im Produkt hinterlegt. Ein Aktivierungscode muss daher nicht angegeben werden. Der hinterlegte Aktivierungscode wird ggf. im Lizenz-Assistenten angezeigt.

Hinweis
Zur Aktivierung des Programms wird eine Verbindung zu den Avira Servern hergestellt. Unter **Proxy Einstellungen** können Sie die Internetverbindung über einen Proxyserver konfigurieren.

- Wählen Sie einen Aktivierungsvorgang und bestätigen Sie mit **Weiter**
- Wenn Sie schon eine gültige Lizenzdatei besitzen, springen Sie zum Abschnitt "Auswahl der Option *Ich habe bereits eine gültige Lizenzdatei*".

Produktaktivierung

↳ Ein Dialogfenster wird geöffnet, in dem Sie Ihre persönlichen Daten eingeben können.

- Geben Sie Ihre Daten ein und klicken Sie auf **Weiter.**

↳ Ihre Daten werden zu den Avira Servern übertragen und geprüft. Ihr Avira Produkt wird mit Ihrer Lizenz aktiviert.

↳ Im folgenden Dialogfenster werden Ihre Lizenzdaten angezeigt.

- Klicken Sie auf **Weiter**.
- Überspringen Sie den folgenden Abschnitt "Auswahl der Option **Ich habe bereits eine gültige Lizenzdatei**".

Auswahl der Option "Ich habe bereits eine gültige Lizenzdatei"

↳ Ein Dialog zum Einlesen der Lizenzdatei wird geöffnet.

- Wählen Sie die Lizenzdatei (in Form einer *.KEY*-Datei) mit Ihren Lizenzdaten für das Programm und klicken Sie auf **Öffnen**.

↳ Im folgenden Dialogfenster werden Ihre Lizenzdaten angezeigt.

- Klicken Sie auf **Weiter**.



Fortsetzung nach abgeschlossener Aktivierung oder Laden der Lizenzdatei

- Die Programmkomponenten werden installiert. Der Installationsfortschritt wird im Dialogfenster angezeigt.

  ↪ Das Dialogfenster **Schließen Sie sich Millionen von Avira-Nutzern an, die bereits Avira SearchFree nutzen** erscheint.

- Wenn Sie die Avira SearchFree Toolbar nicht installieren möchten, entfernen Sie die Markierung aus dem Kästchen der Avira SearchFree Toolbar und Avira SearchFree Updater **Lizenzvereinbarung** und deaktivieren Sie die Festlegung von **Avira SearchFree (search.avira.com)** als Startseite.

> **Hinweis**
> Bitte deinstallieren Sie ggf. bereits installierte Suchleisten vor der Installation der Avira SearchFree Toolbar. Anderenfalls ist eine Installation der Avira SearchFree Toolbar nicht möglich.

- Klicken Sie auf **Weiter**.

  ↪ Der Installationsfortschritt der Avira SearchFree Toolbar wird durch einen grünen Balken dargestellt.

  ↪ Der Installationsassistent wird geschlossen und der Konfigurationsassistent öffnet sich.

3.5 Testprodukt Installation

So installieren Sie Ihr Avira Produkt:

Starten Sie das Installationsprogramm mit einem Doppelklick auf die Installationsdatei, die Sie aus dem Internet heruntergeladen haben, oder legen Sie die Programm-CD ein.

Internetbasierte Installation

↪ Das Dialogfenster **Willkommen** erscheint.

- Klicken Sie auf **Weiter**, um mit der Installation fortzufahren.

  ↪ Das Dialogfenster **Sprachauswahl** erscheint.

- Wählen Sie die Sprache aus, in der Sie Ihr Avira Produkt installieren möchten und bestätigen Sie Ihre Sprachauswahl mit **Weiter**.

  ↪ Das Dialogfenster **Download** erscheint. Alle zur Installation benötigten Dateien werden von den Avira Webservern heruntergeladen. Nach Abschluss des Downloads schließt sich das Fenster **Download**.

Installation mit einem Installationspaket

↪ Das Fenster **Installation wird vorbereitet** erscheint.



↳ Die Installationsdatei wird entpackt. Die Installationsroutine wird gestartet.

↳ Das Dialogfenster **Installationsart wählen** erscheint.

Hinweis
Standardmäßig ist die **Expressinstallation**, bei der die Standardkomponenten ohne Konfigurationsmöglichkeiten installiert werden, voreingestellt. Möchten Sie eine *Benutzerdefinierte Installation* durchführen, lesen Sie bitte hier weiter: Installation und Deinstallation > Benutzerdefinierte Installation.

- Die Option **Ich möchte meinen Schutz mit Avira ProActiv und Cloud-Sicherheit verbessern** ist voreingestellt (Konfiguration > Allgemeines > Erweiteter Schutz). Sie haben die Möglichkeit, an der Avira Community nicht teilzunehmen, indem Sie das Kontrollkästchen deaktivieren.

  ↳ Avira sendet Daten zu verdächtigen Programmen an das Avira Malware Research Center. Die Daten werden allein zu einer erweiterten Onlineprüfung und zur Erweiterung und Verfeinerung der Erkennungstechnologie genutzt. Über die Links **ProActiv** und **Cloud-Sicherheit** können Sie Details zur erweiterten Online-Prüfung abrufen.

- Bestätigen Sie, dass Sie die **Endbenutzer-Lizenzvereinbarung** akzeptieren. Wenn Sie die Details der Lizenzvereinbarung lesen möchten, klicken Sie auf den entsprechenden Link.
- Klicken Sie **Weiter**.

  ↳ Der *Lizenz-Assistent* öffnet sich, mit dessen Hilfe Sie Ihr Produkt aktivieren.

  ↳ Der Assistent bietet Ihnen auch die Möglichkeit, einen Proxyserver festzulegen.

- Klicken Sie **Proxy Einstellungen**, um die notwendige Konfiguration vorzunehmen, und bestätigen Sie mit **OK**.
- Wählen Sie im Lizenz-Assistenten **Produkt testen** und klicken Sie **Weiter**.
- Geben Sie Ihre Daten in den erforderlichen Feldern der Registrierung ein. Entscheiden Sie, ob Sie den *Avira Newsletter* abonnieren möchten und klicken Sie **Weiter**.

  ↳ Der Installationsfortschritt wird durch einen grünen Balken dargestellt.

  ↳ Das Dialogfenster **Schließen Sie sich Millionen von Avira-Nutzern an, die bereits Avira SearchFree nutzen** erscheint.

- Wenn Sie die Avira SearchFree Toolbar nicht installieren möchten, entfernen Sie die Markierung aus den Kästchen der Avira SearchFree Toolbar und Avira SearchFree Updater **Lizenzvereinbarung** und deaktivieren Sie die Festlegung von **Avira SearchFree (search.avira.com)** als Startseite.

Hinweis
Bitte deinstallieren Sie ggf. bereits installierte Suchleisten vor der Installation

der Avira SearchFree Toolbar. Anderenfalls ist eine Installation der Avira SearchFree Toolbar nicht möglich.

- Klicken Sie auf **Weiter**.
  - ↳ Der Installationsfortschritt der Avira SearchFree Toolbar wird durch einen grünen Balken dargestellt.
- Sie werden aufgefordert, einen Neustart auszuführen, um das Avira Produkt zu aktivieren. Klicken Sie **Ja**, um einen sofortigen Neustart anzustoßen.
  - ↳ Das Avira Tray Icon ist in der Taskleiste verankert.
  - ↳ Ihre Testlizenz hat eine Gültigkeit von 31 Tagen.

3.6 Konfigurationsassistent

Bei einer benutzerdefinierten Installation wird am Schluss der Konfigurationsassistent geöffnet. Sie können im Konfigurationsassistenten wichtige Einstellungen für Ihr Avira Produkt vornehmen.

- Klicken Sie im Willkommensfenster des Konfigurationsassistenten auf **Weiter**, um mit der Konfiguration des Programms zu beginnen.
  - ↳ Im Dialogfenster **AHeAD konfigurieren**, können Sie eine Erkennungsstufe für die AHeAD-Technologie wählen. Die gewählte Erkennungsstufe wird für die Einstellung der AHeAD-Technologie des System-Scanners (Direktsuche) und des Echtzeit-Scanners (Echtzeitsuche) übernommen.
- Wählen Sie eine Erkennungsstufe und setzen Sie die Konfiguration mit **Weiter** fort.
  - ↳ Im folgenden Dialogfenster **Erweiterte Gefahrenkategorien wählen**, können Sie mit der Auswahl von Gefahrenkategorien die Schutzfunktionen Ihres Avira Produkts anpassen.
- Aktivieren Sie ggf. weitere Gefahrenkategorien und setzen Sie die Konfiguration mit **Weiter** fort.
  - ↳ Falls Sie das Installationsmodul Avira FireWall zur Installation ausgewählt haben , erscheint das Dialogfenster **Standardregeln für den Zugriff auf das Netzwerk und die Verwendung von Netzwerkressourcen**. Sie können festlegen, ob Avira FireWall externe Zugriffe auf freigegebene Ressourcen sowie Netzzugriffe von Anwendungen vertrauenswürdiger Unternehmen erlaubt.
- Aktivieren Sie die gewünschten Optionen und setzen Sie die Konfiguration mit **Weiter** fort.
  - ↳ Falls Sie das Installationsmodul Avira Echtzeit-Scanner zur Installation ausgewählt haben, erscheint das Dialogfenster **Startmodus des Echtzeit-Scanners**. Sie können den Startzeitpunkt des Echtzeit-Scanners festlegen. Der Echtzeit-Scanner wird bei jedem Neustart des Computers im angegebenen Startmodus gestartet.



Hinweis
Der angegebene Startmodus des Echtzeit-Scanners wird in der Registry hinterlegt und kann nicht über die Konfiguration geändert werden.

Hinweis
Die Auswahl des standardmäßigen Startmodus für den Echtzeit-Scanner (Normaler Start) und ein schnelles Anmelden des Benutzerkontos hat beim Start des Rechners u. U. zur Folge, dass die beim Systemstart automatisch startenden Programme nicht gescannt werden, da diese noch vor dem vollständigen Laden des Echtzeit-Scanners gestartet worden sind.

- Aktivieren Sie die gewünschte Option und setzen Sie die Konfiguration mit **Weiter** fort.
  - ↳ Falls Sie das Installationsmodul Avira Browser-Schutz zur Installation ausgewählt haben, erscheint das Dialogfenster **Sicher Surfen aktivieren**. Sie haben die Möglichkeit, den Benutzern des Rechners verschiedene Rollen für die Internetnutzung (Kind, Jugendlicher, Erwachsener) zuzuweisen. Sie können die Option **Sicher Surfen** auch deaktivieren.
- Nehmen Sie die gewünschten Einstellungen für **Sicher Surfen** vor und setzen Sie die Konfiguration mit **Weiter** fort.
  - ↳ Im folgenden Dialogfenster **Kennwort vergeben**, können Sie den Zugriff auf die Konfiguration mit einem Kennwort schützen. Dies ist besonders bei aktiviertem **Sicher Surfen** empfehlenswert.
  - ↳ Im folgenden Dialogfenster **Systemprüfung** kann die Durchführung einer schnellen Systemprüfung aktiviert oder deaktiviert werden. Die schnelle Systemprüfung wird nach abgeschlossener Konfiguration und vor dem Neustart des Computers ausgeführt und durchsucht gestartete Programme und die wichtigsten Systemdateien nach Viren und Malware.
- Aktivieren oder deaktivieren Sie die Option **Schnelle Systemprüfung** und setzen Sie die Konfiguration mit **Weiter** fort.
  - ↳ Im folgenden Dialogfenster können Sie die Konfiguration mit **Fertig stellen** abschließen.
  - ↳ Die angegebenen und ausgewählten Einstellungen werden übernommen.
  - ↳ Wenn Sie die Option **Schnelle Systemprüfung** aktiviert haben, öffnet sich das Fenster **Luke Filewalker**. Der System-Scanner führt eine schnelle Systemprüfung durch.
  - ↳ Falls Sie nach der Systemprüfung zu einem Systemneustart aufgefordert werden sollten, führen Sie diesen durch, damit Ihr System vollständig geschützt ist.

Nach der erfolgreichen Installation wird empfohlen im Bereich **Status** im Control Center die Aktualität des Schutzprogramms zu prüfen.



- Zeigt Ihr Avira Produkt, dass Ihr Computer nicht vollständig geschützt ist, klicken Sie **Problem beheben**.
  - ↳ Das Dialogfenster **Schutz wiederherstellen** öffnet sich.
- Maximieren Sie die Sicherheit Ihres Systems, indem Sie die vorgegebenen Optionen aktivieren.
- Führen Sie ggf. im Anschluss eine vollständige Systemprüfung durch.

3.7 Änderungsinstallation

Sie haben die Möglichkeit, einzelne Programmkomponenten der aktuellen Installation des Avira Produktes hinzuzufügen oder zu entfernen (siehe Kapitel Installation und Deinstallation > Installationsmodule)

Wenn Sie Programmkomponenten der aktuellen Installation hinzufügen oder entfernen möchten, können Sie in der **Windows-Systemsteuerung** die Option **Software** zum **Ändern/Entfernen** von Programmen verwenden.

Wählen Sie Ihr Avira Produkt aus und klicken Sie auf **Ändern**. Im *Willkommen*-Dialog des Programms wählen Sie die Option **Programm ändern**. Sie werden durch die Änderungsinstallation geführt.

3.8 Installationsmodule

Bei einer benutzerdefinierten Installation oder einer Änderungsinstallation können folgende Module zur Installation ausgewählt oder hinzugefügt bzw. entfernt werden:

- **Avira Internet Security**
  Dieses Modul beinhaltet alle Komponenten, die für eine erfolgreiche Installation Ihres Avira Produkts benötigt werden.
- **Echtzeit-Scanner**
  Der Avira Echtzeit-Scanner läuft im Hintergrund. Er überwacht und repariert, falls möglich, Dateien bei Operationen wie Öffnen, Schreiben und Kopieren in Echtzeit (On-Access = bei Zugriff). Führt ein Benutzer eine Dateioperation durch (Datei laden, ausführen, kopieren), durchsucht das Avira Produkt automatisch die Datei. Bei der Dateioperation Umbenennen wird keine Suche des Avira Echtzeit-Scanners ausgeführt.
- **Email-Schutz**
  Email-Schutz ist die Schnittstelle zwischen Ihrem Computer und dem Email-Server, von dem Ihr Email-Programm (Email-Client) die Emails herunterlädt. Email-Schutz hängt sich als sogenannter Proxy zwischen das Email-Programm und den Email-Server. Alle eingehenden Emails werden durch diesen Proxy geleitet, dabei auf Viren bzw. unerwünschte Programme geprüft und an Ihr Email-Programm weitergeleitet. Je nach Konfiguration behandelt das Programm die betroffenen Emails automatisch oder fragt den Benutzer nach einer bestimmten Aktion. Zusätzlich verfügt der Email-Schutz über die Fähigkeit, Sie zuverlässig vor Spam-Emails zu schützen.



- **Avira FireWall**
  Die Avira FireWall kontrolliert die Kommunikationswege von und zu Ihrem Computer. Sie erlaubt oder verweigert die Kommunikation auf der Basis von Sicherheitsrichtlinien.
- **Rootkits-Schutz**
  Der Avira Rootkits-Schutz prüft, ob sich auf Ihrem Computer bereits Software installiert hat, die nach dem Einbruch in das Computersystem mit den herkömmlichen Methoden der Malware-Erkennung nicht gefunden werden kann.
- **ProActiv**
  Die ProActiv-Komponente überwacht Aktionen von Anwendungen und meldet ein verdächtiges Verhalten von Anwendungen. Mit dieser verhaltensbasierten Erkennung können Sie sich vor unbekannter Malware schützen. Die ProActiv-Komponente ist in den Avira Echtzeit-Scanner integriert.
- **Cloud-Sicherheit**
  Die Cloud-Sicherheit-Komponente ist ein Modul zur dynamischen Online-Erkennung bisher unbekannter Malware.
- **Backup**
  Mit der Komponente Backup können Sie manuell und automatisiert Spiegel-Backups Ihrer Daten erstellen.
- **Browser-Schutz**
  Beim "Surfen" im Internet fordern Sie über Ihren Webbrowser Daten von einem Webserver an. Die vom Webserver übertragenen Daten (HTML-Dateien, Skript- und Bilddateien, Flash-Dateien, Video- und Musik-Streams, etc.) gelangen normalerweise vom Browser-Cache direkt zur Ausführung in den Webbrowser, sodass eine Prüfung durch eine Echtzeitsuche, wie sie der Avira Echtzeit-Scanner zur Verfügung stellt, nicht möglich ist. Auf diesem Weg können Viren und unerwünschte Programme in Ihr Computersystem gelangen. Der Browser-Schutz ist ein sogenannter HTTP-Proxy, der die zur Datenübertragung genutzten Ports (80, 8080, 3128) überwacht und die übertragenen Daten auf Viren und unerwünschte Programme prüft. Je nach Konfiguration behandelt das Programm die betroffenen Dateien automatisch oder fragt den Benutzer nach einer bestimmten Aktion.
- **Shell Extension**
  Die Shell Extension erzeugt im Kontextmenü des Windows Explorers (rechte Maustaste) den Eintrag *Ausgewählte Dateien mit Avira überprüfen*. Mit diesem Eintrag können Sie einzelne Dateien oder Verzeichnisse direkt scannen.

3.9 Deinstallation

Wenn Sie das Avira Produkt von Ihrem Computer entfernen möchten, können Sie die Option **Software** zum **Ändern/Entfernen** von Programmen in der Windows-Systemsteuerung verwenden.

So deinstallieren Sie Ihr Avira Produkt (beschrieben am Beispiel von Windows 7):

- Öffnen Sie über das Windows **Start**-Menü die **Systemsteuerung**.
- Doppelklicken Sie auf **Programme und Funktionen**.

- Wählen Sie Ihr Avira Produkt in der Liste aus und klicken Sie auf **Deinstallieren**.
  - ↬ Sie werden gefragt, ob Sie das Programm tatsächlich entfernen wollen.
- Bestätigen Sie mit **Ja**.
  - ↬ Sie werden gefragt, ob die Windows-Firewall wieder aktiviert werden soll (da die Avira FireWall deaktiviert wird).
- Bestätigen Sie mit **Ja**.
  - ↬ Alle Komponenten des Programms werden entfernt.
- Klicken Sie auf **Fertig stellen**, um die Deinstallation abzuschließen.
  - ↬ Ggf. erscheint ein Dialogfenster mit der Empfehlung, Ihren Computer neu zu starten.
- Bestätigen Sie mit **Ja**.
  - ↬ Das Avira Produkt ist nun deinstalliert, Ihr Computer wird bei Bedarf neu gestartet, dabei werden alle Verzeichnisse, Dateien und Registry-Einträge des Programms gelöscht.

> **Hinweis**
> Die Avira SearchFree Toolbar ist nicht in der Programm-Deinstallation enthalten, sondern muss mithilfe der oben genannten Schritte separat deinstalliert werden. Dazu muss die Avira SearchFree Toolbar über den Add-On Manager aktiviert sein. Nach der Deinstallation ist die Suchleiste nicht länger in Ihren Webbrowser integriert.



4. Überblick über Avira Internet Security

In diesem Kapitel erhalten Sie einen Überblick über die Funktionalitäten und die Bedienung Ihres Avira Produkts.

- siehe Kapitel Oberfläche und Bedienung
- siehe Kapitel Avira SearchFree Toolbar
- siehe Kapitel So wird es gemacht

4.1 Oberfläche und Bedienung

Sie bedienen Ihr Avira Produkt über drei Oberflächenelemente des Programms:

- Control Center: Überwachung und Steuerung des Avira Produkts
- Konfiguration: Konfiguration des Avira Produkts
- Tray Icon im Systemtray der Taskleiste: Öffnen des Control Center und weitere Funktionen

4.1.1 Control Center

Das Control Center dient zur Überwachung des Schutzstatus Ihres Computersystems und zur Steuerung und Bedienung der Schutzkomponenten und Funktionen Ihres Avira Produkts.



Das Fenster des Control Centers gliedert sich in drei Bereiche: Die **Menüleiste**, der **Navigationsbereich** und das Detailfenster **Status**:

- **Menüleiste:** In den Menüs des Control Centers können Sie allgemeine Programmfunktionen aufrufen und Informationen zum Produkt abrufen.
- **Navigationsbereich:** Im Navigationsbereich können Sie einfach zwischen den einzelnen Rubriken des Control Centers wechseln. Die einzelnen Rubriken enthalten Informationen und Funktionen der Programmkomponenten und sind in der Navigationsleiste nach Aufgabenbereichen angeordnet. Beispiel: Aufgabenbereich *PC SICHERHEIT* - Rubrik **Echtzeit-Scanner**.
- **Status:** Im Startbildschirm **Status** sehen Sie auf einen Blick, ob Ihr Computer ausreichend geschützt ist und haben sofort einen Überblick, welche Module aktiv sind, wann das letzte Backup und die letzte Systemprüfung durchgeführt wurden. Im Fenster **Status** befinden sich die Schaltflächen zur Ausführung von Funktionen bzw. Aktionen, wie etwa das Ein- oder Ausschalten des **Echtzeit-Scanners**.

Starten und beenden von Control Center

Sie haben folgende Möglichkeiten das Control Center zu starten:

- Mit Doppelklick auf das Programm-Icon auf Ihrem Desktop

- Über den Programm-Eintrag im Menü **Start > Programme**.
- Über das Tray Icon Ihres Avira Produkts.

Sie beenden das Control Center über den Menübefehl **Beenden** im Menü **Datei**, mit dem Tastaturbefehl **Alt+F4** oder indem Sie auf das Schließen-Kreuz im Control Center klicken.

Control Center bedienen

So navigieren Sie im Control Center:

- Klicken Sie in der Navigationsleiste auf einen Aufgabenbereich unterhalb einer Rubrik.
  - ↳ Der Aufgabenbereich wird mit weiteren Funktions- und Konfigurationsmöglichkeiten im Detailfenster angezeigt.
- Klicken Sie ggf. einen anderen Aufgabenbereich an, um diesen im Detailfenster anzuzeigen.

> **Hinweis**
> Die Tastaturnavigation in der Menüleiste aktivieren Sie mit Hilfe der [**Alt**]-Taste. Ist die Navigation aktiviert, können Sie sich mit den Pfeiltasten innerhalb des Menüs bewegen. Mit der **Enter**-Taste aktivieren Sie den aktuell markierten Menüpunkt.
> Um Menüs im Control Center zu öffnen, zu schließen oder in den Menüs zu navigieren können Sie auch Tastenkombinationen verwenden: [**Alt**]-Taste + unterstrichener Buchstabe im Menü oder Menübefehl. Halten Sie die [**Alt**]-Taste gedrückt, wenn Sie aus einem Menü einen Menübefehl oder ein Untermenü aufrufen möchten.

So bearbeiten Sie Daten oder Objekte, die im Detailfenster angezeigt werden:

- Markieren Sie die Daten oder Objekte, die Sie bearbeiten möchten.

  Um mehrere Elemente zu markieren, halten Sie die **Strg**-Taste oder die **Umsch**-Taste (Auswahl untereinander stehender Elemente) gedrückt, während Sie die Elemente auswählen.
- Klicken Sie auf die gewünschte Schaltfläche in der oberen Leiste des Detailfensters, um das Objekt zu bearbeiten.

Control Center im Überblick

- **Status**: Im Startbildschirm **Status** finden Sie alle Rubriken, mit denen Sie die Funktionsfähigkeit des Programms überwachen können (siehe Status).
  - Das Fenster **Status** bietet die Möglichkeit auf einen Blick zu sehen, welche Module aktiv sind und gibt Informationen über das letzte durchgeführte Update.
- *PC SICHERHEIT*: Hier finden Sie die Komponenten, mit denen Sie Dateien auf Ihrem Computersystem auf Viren und Malware prüfen.



  - Die Rubrik **System-Scanner** bietet Ihnen die Möglichkeit, die Direktsuche auf einfache Art und Weise zu konfigurieren bzw. zu starten (siehe System-Scanner). Vordefinierte Profile ermöglichen einen Suchlauf mit bereits angepassten Standardoptionen. Genau so ist es möglich mit Hilfe der Manuellen Auswahl (wird gespeichert) bzw. durch die Erstellung benutzerdefinierter Profile, die Suche nach Viren und unerwünschten Programmen auf Ihre persönlichen Bedürfnisse anzupassen.
  - Die Rubrik Echtzeit-Scanner zeigt Ihnen Informationen zu überprüften Dateien, sowie weitere statistische Daten, welche jederzeit zurückgesetzt werden können und ermöglicht das Aufrufen der Reportdatei. Detailliertere Informationen zum zuletzt gefundenen Virus oder unerwünschten Programm erhalten Sie quasi "per Knopfdruck".
  - Unter der Rubrik **Backup** können Sie einfach und schnell Backups Ihrer Daten erstellen und Backup-Aufträge anlegen (siehe Backup).

- *INTERNET SICHERHEIT*: Hier finden Sie die Komponenten, mit denen Sie Ihr Computersystem vor Viren und Malware aus dem Internet sowie vor unerwünschten Netzzugriffen schützen.

  - Die Rubrik **FireWall** bietet Ihnen die Möglichkeit, die Grundeinstellungen der Avira FireWall zu konfigurieren. Es werden Ihnen außerdem die aktuelle Datenübertragungsrate und alle aktiven Anwendungen angezeigt, die eine Netzwerkverbindung verwenden (siehe FireWall).
  - Die Rubrik Browser-Schutz zeigt Ihnen Informationen zu überprüften URLs und gefundenen Viren, sowie weitere statistische Daten, welche jederzeit zurückgesetzt werden können und ermöglicht das Aufrufen der Reportdatei. Detailliertere Informationen zum zuletzt gefundenen Virus oder unerwünschten Programm erhalten Sie quasi "per Knopfdruck".
  - Die Rubrik **Email-Schutz** zeigt Ihnen die überprüften Emails, deren Eigenschaften sowie weitere statistische Daten. Zudem haben Sie die Möglichkeit den AntiSpam-Filter zu trainieren und Email-Adressen zukünftig von der Überprüfung auf Malware bzw. Spam auszuschließen. Emails können auch aus dem Email-Schutz-Zwischenspeicher gelöscht werden. (siehe Email-Schutz).

- *KINDER SCHUTZ*: Hier finden Sie Werkzeuge, mit denen Sie ein sicheres Web-Erlebnis für Ihre Kinder ermöglichen.

  - Soziale Netzwerke: Die Rubrik Soziale Netzwerke leitet Sie zur Avira Kinderschutz für soziale Netzwerke Anwendung weiter. Avira Kinderschutz für soziale Netzwerke informiert Eltern über die Online-Aktivitäten ihrer Kinder. Das System prüft die Konten der sozialen Netzwerke auf Kommentare, Fotos usw., die dem Ruf ihres Kindes schaden könnten oder die darauf hinweisen könnten, dass Ihr Kind gefährdet ist.
  - Sicher Surfen: Den Benutzern des Computers können Nutzerrollen zugewiesen werden. Eine Nutzerrolle ist konfigurierbar und umfasst ein Regelset mit folgenden Kriterien: Verbotene oder erlaubte URLs (Internetadressen), Verbotene Inhaltskategorien, Nutzungsdauer des Internets und ggf. erlaubte Nutzungszeiträume für Wochentage

- *MOBILER SCHUTZ*: Über die Kategorie Avira Free Android Security können Sie online auf Ihre Android-Geräte zugreifen.



  - Mit Avira Free Android Security verwalten Sie all Ihre Geräte, die mit dem Android-Betriebssystem arbeiten.

- *VERWALTUNG*: Hier finden Sie Werkzeuge, mit denen Sie verdächtige oder von Viren betroffene Dateien isolieren und administrieren sowie wiederkehrende Aufgaben planen können.
  - Hinter der Rubrik **Quarantäne** verbirgt sich der so genannte Quarantänemanager. Die zentrale Stelle für bereits in Quarantäne gestellte Dateien oder aber für verdächtige Dateien, die Sie in Quarantäne stellen möchten (siehe Quarantäne). Zudem besteht die Möglichkeit, eine ausgewählte Datei per Email an das Avira Malware Research Center zu senden.
  - Die Rubrik **Planer** bietet Ihnen die Möglichkeit, zeitlich gesteuerte Prüf- und Update-Aufträge sowie Backup-Aufträge zu erstellen und bestehende Aufträge anzupassen bzw. zu löschen (siehe Planer).
  - Die Rubrik **Berichte** bietet Ihnen die Möglichkeit, sich die Ergebnisse der durchgeführten Aktionen anzusehen (siehe Berichte).
  - Die Rubrik **Ereignisse** bietet Ihnen die Möglichkeit, sich über die Ereignisse zu informieren, die von den Modulen des Programms erzeugt werden (siehe Ereignisse).

4.1.2 Spielmodus

Wenn Sie auf Ihrem Computer Anwendungen ausführen, die den Vollbildmodus benötigen, können Sie durch Aktivierung des Spielmodus Desktop-Mitteilungen und Hinweise wie Popup-Fenster und Produkt-Benachrichtigungen gezielt unterdrücken. Im Spielmodus werden alle definierten Adapter- und Anwendungsregeln, die Sie in der Konfiguration der Avira FireWall vorgenommen haben, angewendet, ohne dass Sie zu Netzwerkereignissen benachrichtigt werden.

Sie haben die Möglichkeit, den Spielmodus mit einem Klick auf die Schaltfläche **AN/AUS** zu aktivieren bzw. im automatischen Modus zu halten. Voreingestellt ist der Spielmodus mit **Automatik** und wird in grüner Farbe dargestellt. Mit dieser Voreinstellung schaltet Ihr Avira Produkt automatisch auf den Spielmodus um, wenn Sie eine Anwendung im Vollbildmodus ausführen.

- Klicken Sie die Schaltfläche links neben **AUS**, um den Spielmodus zu aktivieren.
  - ↳ Der Spielmodus ist eingeschaltet, und die Schaltfläche wird in gelber Farbe dargestellt.

> **Hinweis**
> Wir empfehlen, den voreingestellten Status **AUS** mit seiner automatischen Erkennung von Anwendungen im Vollbildmodus nur temporär zu ändern, da Sie im Spielmodus keine sichtbaren Desktop-Mitteilungen und Warnungen über Netzwerkzugriffe und eventuelle Gefahren erhalten.

4.1.3 Konfiguration

In der Konfiguration können Sie Einstellungen für Ihr Avira Produkt vornehmen. Nach der Installation ist Ihr Avira Produkt mit Standardeinstellungen konfiguriert, die gewährleisten, dass Ihr Computersystem optimal geschützt ist. Dennoch können Ihr Computersystem oder Ihre Anforderungen an Ihr Avira Produkt Besonderheiten aufweisen, so dass Sie die Schutzkomponenten des Programms anpassen möchten.

Die Konfiguration hat den Aufbau eines Dialogfensters: Mit den Schaltflächen **OK** oder **Übernehmen** speichern Sie Ihre in der Konfiguration vorgenommenen Einstellungen, mit **Abbrechen** verwerfen Sie Ihre Einstellungen, mit der Schaltfläche **Standardwerte** können Sie die Einstellungen in der Konfiguration auf die Standardwerte zurücksetzen. In der linken Navigationsleiste können Sie einzelne Konfigurationsrubriken anwählen.

Aufrufen der Konfiguration

Sie haben mehrere Möglichkeiten die Konfiguration aufzurufen:

- Über die Windows Systemsteuerung.
- Über das Windows Sicherheitscenter - ab Windows XP Service Pack 2.
- Über das Tray Icon Ihres Avira Programms.
- Im Control Center über den Menüpunkt Extras > Konfiguration.

- Im Control Center über die Schaltfläche Konfiguration.

> **Hinweis**
> Wenn Sie die Konfiguration über die Schaltfläche **Konfiguration** im Control Center aufrufen, gelangen Sie in das Konfigurationsregister der Rubrik, die im Control Center aktiv ist.

Konfiguration bedienen

Sie navigieren innerhalb des Konfigurationsfensters wie im Windows Explorer:

- Klicken Sie einen Eintrag in der Baumstruktur an, um diese Konfigurationsrubrik im Detailfenster anzuzeigen.
- Klicken Sie auf das Plus-Zeichen vor einem Eintrag, um die Konfigurationsrubrik zu erweitern und untergeordnete Konfigurationsrubriken in der Baumstruktur anzuzeigen.
- Um untergeordnete Konfigurationsrubriken zu verbergen, klicken Sie auf das Minus-Zeichen vor der erweiterten Konfigurationsrubrik.

> **Hinweis**
> Um in der Konfiguration Optionen zu aktivieren oder deaktivieren und Schaltflächen zu drücken, können Sie auch die Tastenkombinationen verwenden: [**Alt**]-Taste + unterstrichener Buchstabe im Optionsnamen oder der Schaltflächenbezeichnung.

Wenn Sie Ihre Einstellungen in der Konfiguration übernehmen möchten:

- Klicken Sie auf die Schaltfläche **OK**.
  - ↳ Das Konfigurationsfenster wird geschlossen und die Einstellungen werden übernommen.

  - ODER -

  Klicken Sie auf die Schaltfläche **Übernehmen**.
  - ↳ Die Einstellungen werden übernommen. Das Konfigurationsfenster bleibt geöffnet.

Wenn Sie die Konfiguration beenden möchten ohne Ihre Einstellungen zu übernehmen:

- Klicken Sie auf die Schaltfläche **Abbrechen**.
  - ↳ Das Konfigurationsfenster wird geschlossen, und die Einstellungen werden verworfen.

Wenn Sie alle Einstellungen in der Konfiguration auf Standardwerte zurücksetzen möchten:

▶ Klicken Sie auf **Standardwerte**.

↳ Alle Einstellungen in der Konfiguration werden auf Standardwerte zurückgesetzt. Alle Änderungen und alle eigenen Einträge gehen beim Zurücksetzen auf die Standardwerte verloren.

Konfigurationsoptionen im Überblick

Sie haben folgende Konfigurationsoptionen:

- **System-Scanner**: Konfiguration der Direktsuche
  - Suchoptionen
  - Aktion bei Fund
  - Optionen bei Suche in Archiven
  - Ausnahmen der Direktsuche
  - Heuristik der Direktsuche
  - Einstellung der Reportfunktion
- **Echtzeit-Scanner**: Konfiguration der Echtzeitsuche
  - Suchoptionen
  - Aktion bei Fund
  - Weitere Aktionen
  - Ausnahmen der Echtzeitsuche
  - Heuristik der Echtzeitsuche
  - Einstellung der Reportfunktion
- **Backup**:
  - Einstellung der Backup-Komponente (Inkrementelles Backup, Suche nach Viren bei Backup)
  - Ausnahmen: Einstellung der zu sichernden Dateien
  - Einstellung der Reportfunktion
- **Update**: Konfigurationen der Update-Einstellungen
- **FireWall**: Konfiguration der FireWall
  - Einstellung von Adapterregeln
  - Benutzerdefinierte Einstellung von Anwendungsregeln
  - Liste vertrauenswürdiger Anbieter (Ausnahmen beim Netzzugriff von Anwendungen)
  - Erweiterte Einstellungen: Zeitüberschreitung von Regeln, Windows FireWall stoppen, Benachrichtigungen
  - Popup-Einstellungen (Warnmeldungen beim Netzzugriff von Anwendungen)
- **Browser-Schutz**: Konfiguration des Browser-Schutzes
  - Suchoptionen, Aktivierung und Deaktivierung des Browser-Schutzes
  - Aktion bei Fund
  - Gesperrte Zugriffe: Unerwünschte Dateitypen und MIME-Typen, Web-Filter für bekannte unerwünschte URLS (Malware, Phishing etc.)

- Ausnahmen der Suche des Browser-Schutzes: URLs, Dateitypen, MIME-Typen
- Heuristik des Browser-Schutzes
- Einstellung der Reportfunktion

- **Email-Schutz**: Konfiguration des Email-Schutzes
  - Suchoptionen: Aktivierung der Überwachung von POP3-Konten, IMAP-Konten, ausgehenden Emails (SMTP)
  - Aktion bei Fund
  - Weitere Aktionen
  - Heuristik der Suche des Email-Schutzes
  - AntiBot-Funktion: Erlaubte SMTP-Server, erlaubte Email-Absender
  - Ausnahmen der Suche des Email-Schutzes
  - Konfiguration des Zwischenspeichers, Zwischenspeicher leeren
  - Konfiguration der AntiSpam-Trainingsdatenbank, Trainingsdatenbank leeren
  - Konfiguration einer Fußzeile in gesendeten Emails
  - Einstellung der Reportfunktion
- **Kinder Schutz**:
  - Sicher Surfen: Kinderschutzfunktion mit rollenbasiertem Filter und mit rollenbasierter Zeitbeschränkung der Internetnutzung
- **Allgemeines**:
  - Erweiterte Gefahrenkategorien für Direkt- und Echtzeitsuche
  - Erweiterter Schutz: ProActiv und Cloud-Sicherheit aktivieren
  - Anwendungsfilter: Anwendungen blockieren oder erlauben
  - Kennwortschutz für den Zugriff auf das Control Center und die Konfiguration
  - Sicherheit: Autorun Funktionen blockieren, Windows hosts-Datei sperren, Produktschutz
  - WMI: WMI-Unterstützung aktivieren
  - Konfiguration der Ereignis-Protokollierung
  - Konfiguration der Bericht-Funktionen
  - Einstellung der verwendeten Verzeichnisse
  - Konfiguration von akustischen Warnungen bei Malware-Fund

4.1.4 Tray Icon

Nach der Installation sehen Sie das Tray Icon Ihres Avira Produkts im Systemtray der Taskleiste:

Symbol	Beschreibung
	Avira Echtzeit-Scanner ist aktiviert und die FireWall ist aktiviert
	Avira Echtzeit-Scanner ist deaktiviert oder die FireWall ist deaktiviert

Das Tray Icon zeigt den Status des Echtzeit-Scanners und der FireWall an.

Über das Kontextmenü des Tray Icons sind zentrale Funktionen Ihres Avira Produkts schnell zugänglich.

- Um das Kontextmenü aufzurufen, klicken Sie mit der rechten Maustaste auf das Tray Icon.

Einträge im Kontextmenü

- **Echtzeit-Scanner aktivieren**: Aktiviert bzw. deaktiviert den Avira Echtzeit-Scanner.
- **Email-Schutz aktivieren**: Aktiviert bzw. deaktiviert den Avira Email-Schutz.
- **Browser-Schutz aktivieren**: Aktiviert bzw. deaktiviert den Avira Browser-Schutz.
- **FireWall**:
  - **FireWall aktivieren**: Aktiviert bzw. deaktiviert die Avira FireWall
  - **Gesamten Verkehr blockieren**: Aktiviert: Blockiert jede Datenübertragung mit Ausnahme von Übertragungen zum eigenen Computersystem (Local Host / IP 127.0.0.1).
- **Avira Internet Security starten**: Öffnet das Control Center.
- **Avira Internet Security konfigurieren**: Öffnet die Konfiguration.
- **Meine Meldungen**: Öffnet ein Slide-Up mit aktuellsten Meldungen zu Ihrem Avira Produkt.
- **Meine Kommunikationseinstellungen**: Öffnet das Abo-Center für Produktmitteilungen
- **Update starten**: Startet ein Update.
- **Hilfe**: Öffnet die Online-Hilfe.
- **Experts Market**: öffnet die Webseite Experts Market - Hilfe anfordern. Dort können Sie um Hilfe bitten oder anderen Anwendern Ihre Hilfe anbieten.
- **Über Avira Internet Security:** Öffnet ein Dialogfenster mit Informationen zu Ihrem Avira Produkt: Produktinformationen, Versionsinformationen, Lizenzinformationen.
- **Avira im Internet**: Öffnet das Avira Webportal im Internet. Voraussetzung ist, dass Sie einen aktiven Zugang zum Internet haben.

Hinweis
Die Benutzerkontensteuerung (UAC) benötigt Ihre Zustimmung zur Aktivierung oder Deaktivierung der Echtzeit-Scanner, FireWall, Browser-Schutz und Email-Schutz Dienste in Betriebssystemen ab Windows Vista.

4.2 Avira SearchFree Toolbar

Avira SearchFree Toolbar beinhaltet zwei Hauptkomponenten: Avira SearchFree und die schon bekannte Toolbar.

Die neue Avira SearchFree Toolbar wird als ein Add-on installiert. Beim ersten Aufrufen des Browsers (bei Internet Explorer und Firefox) werden Sie gefragt, ob Sie zulassen möchten, dass das Programm Avira SearchFree Toolbar Ihren Browser modifiziert. Sie müssen akzeptieren, um eine erfolgreiche Installation von Avira SearchFree Toolbar abzuschließen.

Avira SearchFree ist die neue Suchmaschine von Avira und enthält ein klickbares Avira Logo, das zu der Avira Webseite führt, sowie Web- und Bildkanäle. Sie ermöglicht Avira-Benutzern eine umfangreiche und sichere Suche.

Die Toolbar wird in Ihren Webbrowser integriert und besteht aus einem Suchfeld, einem mit der Avira Webseite verlinkten Avira Logo, zwei Statusanzeigen, drei Widgets und dem Menü **Optionen**.

- Suchleiste
  Nutzen Sie die Suchleiste, um schnell und kostenlos mithilfe der Avira SearchFree Suchmaschine das Internet zu durchsuchen.
- Statusanzeige
  Die Statusanzeigen geben Aufschluss über den Status des Browser-Schutzes und den aktuellen Update-Status Ihres Avira Produkts und helfen Ihnen, zu erkennen, welche Aktionen Sie ggf. zum Schutz Ihres PCs durchführen sollten.
- Widgets
  Avira gibt Ihnen direkten Zugang zu wichtigen Funktionen rund ums Internet, z.B. Ihre Facebook-Nachrichten oder Ihr Email-Postfach. Sie können auch die Sicherheit Ihres Systems durch das Widget Browser-Sicherheit bestimmen (nur Firefox und Internet Explorer).
- Optionen
  Mithilfe des Optionen-Menüs können Sie auf die Toolbar-Optionen zugreifen, den Suchverlauf löschen, Hilfe und Informationen zur Toolbar aufrufen und die Avira SearchFree Toolbar auch direkt über den Webbrowser deinstallieren (nur Firefox und Internet Explorer).

4.2.1 Verwendung

Suchleiste

Mithilfe der Suchleiste können Sie das Internet nach einem oder mehreren beliebigen Begriffen durchsuchen.

Geben Sie dafür den Begriff in das Suchfeld ein und drücken Sie danach die **Enter**-Taste oder klicken Sie auf **Suche**. Die Avira SearchFree Suchmaschine durchsucht nun das Internet für Sie und zeigt dann alle Treffer im Browser-Fenster an.

Wie Sie Avira SearchFree im Internet Explorer, Firefox und Chrome Ihren Wünschen entsprechend konfigurieren können, finden Sie unter **Optionen.**

Statusanzeige

Browser-Schutz

Zur Bestimmung des Sicherheitsstatus Ihres Computers, können Sie folgende Icons und Meldungen nutzen:

Symbol	Statusanzeige	Beschreibung
✔	*Browser-Schutz*	Wenn Sie mit dem Mauszeiger über das Symbol fahren, erhalten Sie folgende Meldung: *Avira Browser-Schutz ist aktiv. Sie können jetzt sicher im Internet surfen.* Das bedeutet, dass keine weiteren Aktionen erforderlich sind.
!	*Browser-Schutz*	Wenn Sie mit dem Mauszeiger über das Symbol fahren, erhalten Sie folgende Meldung: *Avira Browser-Schutz ist deaktiviert. Klicken Sie auf den Link, um zu erfahren, wie Sie ihn aktivieren können.* ↳ Sie werden auf einen Artikel unserer Wissensdatenbank weitergeleitet.

	Kein Browser-Schutz	Wenn Sie mit dem Mauszeiger über das Symbol fahren, erhalten Sie folgende Meldung: • *Sie haben Avira Browser-Schutz noch nicht installiert. Klicken Sie auf den Link, um mehr darüber zu erfahren, wie Sie sicher im Internet surfen können.* Das bedeutet, dass Sie entweder Avira Antivirus deinstalliert haben oder, dass es nicht richtig installiert wurde. • *Browser-Schutz ist kostenlos in Avira Antivirus enthalten. Klicken Sie auf den Link, um mehr über seine Installation zu erfahren.* Das bedeutet, dass Sie Browser-Schutz nicht installiert, oder deinstalliert haben. ↪ In beiden Fällen werden Sie auf die Avira Webseite weitergeleitet, von der Sie Ihr Avira Produkt herunterladen können.
	Fehler	Wenn Sie mit dem Mauszeiger über das Symbol fahren, erhalten Sie folgende Meldung: *Avira hat einen Fehler gemeldet.* ▸ Klicken Sie auf das graue Symbol oder den Text, um zur Avira Support-Seite zu gelangen.

Widgets

Avira SearchFree Toolbar verfügt über 3 Widgets mit den wichtigsten Funktionen rund ums Internet: Facebook, Email und Browser-Sicherheit.

Facebook

Diese Funktion ermöglicht Ihnen, die Mitteilungen von Facebook direkt zu erhalten und so auf dem neuesten Stand zu bleiben.

Email

Wenn Sie auf das Email Symbol klicken, bekommen Sie eine Dropdown-Liste angezeigt, in der Sie zwischen den meistverwendeten Anbietern wählen können.

Browser-Sicherheit

Dieses Widget wurde von Avira entwickelt, um alle Internet-Sicherheitsoptionen besonders leicht erreichbar zu machen. Zur Zeit ist es nur für Firefox und Internet Explorer verfügbar. Es werden verschiedene Optionen angeboten, die je nach Browser anders heißen können:

- *Pop-up-Blocker*

Ist diese Option eingeschaltet, werden alle Pop-up-Fenster blockiert, wenn Sie im Internet surfen.

- *Cookie-Blocker*

Ist diese Option aktiviert, werden während des Browsens keine Cookies gespeichert.

- *Privater Modus (Firefox) / In Private Browsen (Internet Explorer)*

Ist diese Option eingeschaltet, hinterlassen Sie keine Spuren, wenn Sie im Internet surfen. Diese Option wird nicht für Internet Explorer 7 und 8 angeboten.

- *Neueste Chronik löschen (Firefox) / Browserverlauf löschen (Internet Explorer)*

Mit dieser Option löschen Sie alle Ihre bisherigen Internetaktivitäten.

Sicherheitsberater

Der Sicherheitsberater bietet Ihnen eine Sicherheitseinstufung während Sie im Internet navigieren.
So können Sie abschätzen, ob die Webseite die Sie gerade besuchen, ein hohes oder ein niedriges Risiko für Ihre Sicherheit birgt.
Dieses Widget bietet Ihnen weitere Informationen über die Webseite, wie z.B. wer der Domain-Besitzer ist oder warum eine Webseite in eine bestimmte Kategorie eingestuft wurde.

Die Sicherheitsstufen werden in der Toolbar und in Ihren Suchergebnissen angezeigt, dargestellt in Form eines Avira Tray Icon mit verschiedenen Symbolen:

Symbol	Statusanzeige	Beschreibung
	Sicher	Ein grünes Häkchen für sichere Webseiten.
	Risikoarm	in gelbes Ausrufezeichen für Webseiten, die ein geringes Risiko darstellen.



	Risikoreich	Ein rotes Stopp-Schild für Webseiten, die ein hohes Risiko für Ihre Sicherheit bergen.
	Gescheitert	Ein graues Fragezeichen für Webseiten, deren Risiko nicht eingeschätzt werden kann.
	Überprüfung läuft	Dieses Zeichen wird erscheinen, während der Status verifiziert wird.

Spurenblocker

Mit dem Spurenblocker können Sie Nachverfolgungen stoppen, die Informationen über Sie sammeln während Sie im Internet surfen.
Das Widget erlaubt Ihnen zu wählen, welche Nachverfolgungen blockiert und welche zugelassen werden.

Die Unternehmen sind in drei Kategorien eingeteilt:

- Soziale Netzwerke
- Netzwerke
- Andere Unternehmen

4.2.2 Optionen

Die Avira SearchFree Toolbar ist mit Internet Explorer, Firefox und Google Chrome kompatibel und lässt sich in den Webbrowsern Ihren Wünschen entsprechend konfigurieren:

- Internet Explorer Konfigurationsoptionen
- Firefox Konfigurationsoptionen
- Chrome Konfigurationsoptionen

Internet Explorer

Im Internet Explorer Webbrowser stehen im Menü **Optionen** folgende Konfigurationsoptionen für die Avira SearchFree Toolbar zur Verfügung:

Toolbar-Optionen

Suche

Avira-Suchmaschine

Im Menü **Avira-Suchmaschine** können Sie auswählen, welche Suchmaschine für die Suchanfrage verwendet werden soll. Zur Verfügung stehen Suchmaschinen aus den

USA, Brasilien, Deutschland, Spanien, Europa, Frankreich, Italien, den Niederlanden, Russland und Großbritannien.

Suche öffnen in

Im Menü der Option **Suche öffnen in** können Sie auswählen, wo das Ergebnis einer Suchanfrage angezeigt werden soll, ob im **Aktuellen Fenster**, in einem **Neuen Fenster** oder auf einer **Neuen Registerkarte**.

Letzte Suchanfragen anzeigen

Ist die Option **Letzte Suchanfragen anzeigen** aktiviert, können Sie sich unterhalb des Texteingabefeldes der Suchleiste die bisher eingegebenen Suchbegriffe anzeigen lassen.

Suchverlauf beim Schließen des Browsers löschen

Aktivieren Sie die Option **Suchverlauf beim Schließen des Browsers löschen**, wenn Sie den Suchverlauf der bereits durchgeführten Suchen nicht speichern, sondern mit dem Schließen des Webbrowsers löschen möchten.

Weitere Optionen

Toolbar-Sprache

Unter **Toolbar-Sprache** können Sie die Sprache auswählen, in der die Avira SearchFree Toolbar angezeigt werden soll. Zur Verfügung stehen Englisch, Deutsch, Spanisch, Französisch, Italienisch, Portugiesisch und Niederländisch.

> **Hinweis**
> Die voreingestellte Sprache der Avira SearchFree Toolbar entspricht der Ihres Programmes, soweit verfügbar. Steht die Toolbar in Ihrer Sprache nicht zur Verfügung, ist die voreingestellte Sprache Englisch.

Schaltflächenbeschriftungen anzeigen

Deaktivieren Sie die Option **Schaltflächenbeschriftungen anzeigen**, wenn Sie den Text neben den Icons der Avira SearchFree Toolbar ausblenden möchten.

Suchverlauf löschen

Aktivieren Sie die Option **Suchverlauf löschen**, wenn Sie die bereits durchgeführte(n) Suche(n) nicht speichern, sondern sofort löschen möchten.

Hilfe

Klicken Sie auf **Hilfe**, um die Webseite mit den häufig gestellten Fragen (FAQ) zur Toolbar aufzurufen.



Deinstallieren

Sie können die Avira SearchFree Toolbar auch direkt im Internet Explorer deinstallieren: Deinstallation über den Webbrowser.

Info

Klicken Sie auf **Info**, um angezeigt zu bekommen, welche Version der Avira SearchFree Toolbar installiert ist.

Firefox

Im Firefox Webbrowser stehen im Menü **Optionen** folgende Konfigurationsoptionen für die Avira SearchFree Toolbar zur Verfügung:

Toolbar-Optionen

Suche

Avira-Suchmaschine

Im Menü **Avira-Suchmaschine** können Sie auswählen, welche Suchmaschine für die Suchanfrage verwendet werden soll. Zur Verfügung stehen Suchmaschinen aus den USA, Brasilien, Deutschland, Spanien, Europa, Frankreich, Italien, den Niederlanden, Russland und Großbritannien.

Letzte Suchanfragen anzeigen

Ist die Option **Letzte Suchanfragen anzeigen** aktiviert, können Sie sich die bisher eingegebenen Suchbegriffe anzeigen lassen, indem Sie auf den Pfeil in der Suchleiste klicken. Wählen Sie einen der Begriffe aus, wenn Sie sich das Suchergebnis erneut anzeigen lassen wollen.

Suchverlauf beim Schließen des Browsers löschen

Aktivieren Sie die Option **Suchverlauf beim Schließen des Browsers löschen**, wenn Sie den Suchverlauf der bereits durchgeführten Suchen nicht speichern, sondern mit dem Schließen des Webbrowsers löschen möchten.

Suchergebnisse von Ask anzeigen, wenn ich Stichwörter oder ungültige URL-Adressen in das Adressfeld des Browsers eingebe

Ist diese Option aktiviert, wird jedes Mal, wenn Sie Stichwörter oder eine ungültige URL-Adresse in das Adressfeld des Webbrowsers eintragen, eine Suchanfrage gestartet und das Suchergebnis angezeigt.

Weitere Optionen

Toolbar-Sprache

Unter **Toolbar-Sprache** können Sie die Sprache auswählen, in der die Avira SearchFree Toolbar angezeigt werden soll. Zur Verfügung stehen Englisch, Deutsch, Spanisch, Französisch, Italienisch, Portugiesisch und Niederländisch.

Hinweis
Die voreingestellte Sprache der Avira SearchFree Toolbar entspricht der Ihres Programmes, soweit verfügbar. Steht die Toolbar in Ihrer Sprache nicht zur Verfügung, ist die voreingestellte Sprache Englisch.

Schaltflächenbeschriftungen anzeigen

Deaktivieren Sie die Option **Schaltflächenbeschriftungen anzeigen**, wenn Sie den Text neben den Icons der Avira SearchFree Toolbar ausblenden möchten.

Suchverlauf löschen

Aktivieren Sie die Option **Suchverlauf löschen**, wenn Sie die bereits durchgeführte(n) Suche(n) nicht speichern, sondern sofort löschen möchten.

Hilfe

Klicken Sie auf **Hilfe**, um die Webseite mit den häufig gestellten Fragen (FAQ) zur Toolbar aufzurufen.

Deinstallieren

Sie können die Avira SearchFree Toolbar auch direkt im Internet Explorer deinstallieren: Deinstallation über den Webbrowser.

Info

Klicken Sie auf **Info**, um angezeigt zu bekommen, welche Version der Avira SearchFree Toolbar installiert ist.

Chrome

Im Google Chrome Webbrowser finden Sie alle Konfigurationsoptionen unterhalb des roten Avira-Schirms. Folgende Optionen stehen für die Avira SearchFree Toolbar zur Verfügung:

Hilfe

Klicken Sie auf **Hilfe**, um die Webseite mit den häufig gestellten Fragen (FAQ) zur Toolbar aufzurufen.

Anweisungen zum Deinstallieren

Hier finden Sie Links zu Deinstallationsanweisungen für Avira SeachFree Toolbar.

Info

Klicken Sie auf **Info**, um angezeigt zu bekommen, welche Version der Avira SearchFree Toolbar installiert ist.

Avira SearchFree Toolbar ein- und ausblenden

Dieser Menüpunkt schaltet die Avira SearchFree Toolbar, die sich im oberen Teil des Fensters befindet, ein- und aus.

4.2.3 Deinstallation

So deinstallieren Sie Ihre Avira SearchFree Toolbar (beschrieben am Beispiel von Windows 7):

- Öffnen Sie über das Windows **Start**-Menü die **Systemsteuerung**.
- Doppelklicken Sie auf **Programme und Funktionen**.
- Wählen Sie **Avira SearchFree Toolbar plus Browser-Schutz** in der Liste aus und klicken Sie auf **Deinstallieren**.
  - ↳ Sie werden gefragt, ob Sie dieses Produkt wirklich deinstallieren wollen.
- Bestätigen Sie mit **Ja**.
  - ↳ Avira SearchFree Toolbar plus Browser-Schutz wird deinstalliert, Ihr Computer wird bei Bedarf neu gestartet, dabei werden alle Verzeichnisse, Dateien und Registry-Einträge der Avira SearchFree Toolbar plus Browser-Schutz gelöscht.

Deinstallation über den Webbrowser

Sie haben außerdem die Möglichkeit, die Avira SearchFree Toolbar in **Firefox und Internet Explorer** direkt im Browser zu deinstallieren:

- Öffnen Sie rechts in der Suchleiste das **Optionen**-Menü.
- Klicken Sie auf **Deinstallieren**.
  - ↳ Wenn Sie Ihren Webbrowser noch geöffnet haben, werden Sie nun aufgefordert, ihn zu schließen.
- Schließen Sie den Webbrowser und klicken Sie auf **OK**.
  - ↳ Avira SearchFree Toolbar plus Browser-Schutz wird deinstalliert, Ihr Computer wird bei Bedarf neu gestartet, dabei werden alle Verzeichnisse, Dateien und Registry-Einträge der Avira SearchFree Toolbar plus Browser-Schutz gelöscht.

> **Hinweis** Beachten Sie, dass für eine Deinstallation der Avira SearchFree Toolbar die Toolbar im Add-Ons Manager aktiviert sein muss.



Deinstallation als Add-On

Da die neueste Version der Avira SearchFree Toolbar als Add-On installiert wird, ist es auch möglich das Tool mit verschiedenen Add-On Managern zu verwalten.

Firefox

Klicken Sie auf **Tools > Add-ons > Erweiterungen**. Dort können Sie das Add-on von Avira verwalten: d.h. ein- und ausschalten oder deinstallieren.

Internet Explorer

Klicken Sie auf **Add-ons verwalten > Symbolleisten und Erweiterungen**. Dort können Sie das Add-on von Avira sowohl ein- und ausschalten als auch deinstallieren.

Google Chrome

Mit einem Klick auf **Optionen > Erweiterungen** verwalten Sie das Avira Add-on. Dieses ermöglicht Ihnen, die Toolbar ein- oder auszuschalten oder zu deinstallieren.

4.3 So wird es gemacht

In den "So wird es gemacht" Kapiteln erhalten Sie eine kurze Anleitung zur Lizenz- und Produktaktivierung sowie zu den wichtigsten Funktionen Ihres Avira Produkts. Die ausgewählten, kurzen Beiträge dienen dazu, Ihnen rasch einen Überblick über die Funktionalitäten Ihres Avira Produkts zu verschaffen. Sie ersetzen jedoch nicht die ausführlichen Erklärungen in den einzelnen Kapiteln dieser Hilfe.

4.3.1 Lizenz aktivieren

So aktivieren Sie die Lizenz Ihres Avira Produkts:

Mit der *.KEY*-Lizenzdatei aktivieren Sie Ihre Lizenz für Ihr Avira Produkt. Die Lizenzdatei erhalten Sie von Avira per Email. Die Lizenzdatei enthält die Lizenz für alle Produkte, die Sie bei einem Bestellvorgang bestellt haben.

Wenn Sie Ihr Avira Produkt noch nicht installiert haben:

- Speichern Sie die Lizenzdatei in einem lokalen Verzeichnis auf Ihrem Computer.
- Installieren Sie Ihr Avira Produkt.
- Geben Sie bei der Installation an, wo Sie die Lizenzdatei gespeichert haben.

Wenn Sie Ihr Avira Produkt bereits installiert haben:

- Doppelklicken Sie in Ihrem Dateimanager oder in der Aktivierungs-Email auf die Lizenzdatei und folgen Sie den Bildschirmanweisungen der sich öffnenden Lizenzverwaltung.

- ODER -

Wählen Sie im Control Center Ihres Avira Produkts den Menüpunkt **Hilfe > Lizenzmanagement**

> **Hinweis**
> Ab Windows Vista erscheint das Dialogfenster **Benutzerkontensteuerung**. Melden Sie sich ggf. als Administrator an. Klicken Sie auf **Fortsetzen**.

- Markieren Sie die Lizenzdatei und klicken Sie auf **Öffnen**.
  - ↳ Eine Meldung erscheint.
- Bestätigen Sie mit **OK**.
  - ↳ Die Lizenz ist aktiviert.
- Starten Sie Ihr System ggf. neu.

4.3.2 Produkt aktivieren

Um Ihr Avira Produkt zu aktivieren, haben Sie die folgenden Optionen:

- Aktivierung mit einer gültigen Volllizenz

  Zur Aktivierung des Programms mit einer Volllizenz benötigen Sie einen gültigen Aktivierungscode, über den die Daten Ihrer erworbenen Lizenz erfasst sind. Den Aktivierungscode haben Sie entweder per Email von uns erhalten oder er ist auf der Produktverpackung vermerkt.
- Aktivierung mit einer Evaluationslizenz

  Ihr Avira Produkt wird mit einer automatisch generierten Evaluationslizenz aktiviert, mit der Sie das Avira Produkt in einem begrenzten Zeitraum im vollen Funktionsumfang testen können.

> **Hinweis**
> Zur Produktaktivierung oder zur Beantragung einer Testlizenz benötigen Sie eine aktive Internetverbindung.
> Falls keine Verbindung zu den Avira Servern erstellt werden kann, prüfen Sie ggf. die Einstellungen in der genutzten Firewall: Bei der Produktaktivierung werden Verbindungen über das HTTP-Protokoll und Port 80 (Webkommunikation) und über das Verschlüsselungsprotokoll SSL und Port 443 genutzt. Stellen Sie sicher, dass Ihre Firewall, eingehende und ausgehende Daten nicht blockiert. Prüfen Sie zunächst, ob Sie über Ihren Webbrowser, Webseiten aufrufen können.

So aktivieren Sie Ihr Avira Produkt:

Wenn Sie Ihr Avira Produkt noch nicht installiert haben:

- Installieren Sie Ihr Avira Produkt.
  - ↳ Während der Installation werden Sie aufgefordert, eine Aktivierungsoption zu wählen
- **Produkt aktivieren** = Aktivierung mit einer gültigen Volllizenz
- **Produkt testen** = Aktivierung mit einer Evaluationslizenz
- Geben Sie für eine Aktivierung mit Volllizenz den Aktivierungscode an.
- Bestätigen Sie die Auswahl des Aktivierungsverfahrens mit **Weiter**.
- Geben Sie ggf. Ihre persönlichen Daten für eine Registrierung an und bestätigen Sie mit **Weiter**.
  - ↳ Im folgenden Dialogfenster werden Ihre Lizenzdaten angezeigt. Ihr Avira Produkt wurde aktiviert.
- Fahren Sie mit der Installation fort.

Wenn Sie Ihr Avira Produkt bereits installiert haben:

- Wählen Sie im Control Center den Menüpunkt **Hilfe > Lizenzmanagement**.
  - ↳ Es öffnet sich der Lizenz-Assistent, in dem Sie eine Aktivierungsoption wählen können. Die weiteren Schritte der Produktaktivierung sind identisch mit dem oben dargestellten Ablauf.

4.3.3 Automatisierte Updates durchführen

So legen Sie mit dem Avira Planer einen Auftrag an, mit dem Ihr Avira Produkt automatisiert aktualisiert wird:

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* **> Planer**.
- Klicken Sie auf das Symbol + **Neuen Auftrag mit dem Wizard erstellen**.
  - ↳ Das Dialogfenster **Name und Beschreibung des Auftrags** erscheint.
- Benennen Sie den Auftrag und beschreiben Sie ihn gegebenenfalls.
- Klicken Sie auf **Weiter**.
  - ↳ Das Dialogfenster **Art des Auftrags** wird angezeigt.
- Wählen Sie **Update-Auftrag** aus der Auswahlliste.
- Klicken Sie auf **Weiter**.
  - ↳ Das Dialogfenster **Zeitpunkt des Auftrags** erscheint.
- Wählen Sie, wann das Update ausgeführt werden soll:
- **Sofort**
- **Täglich**
- **Wöchentlich**
- **Intervall**



- **Einmalig**
- **Login**

> **Hinweis**
> Wir empfehlen, regelmäßig und häufig Updates durchzuführen. Das empfohlene Update-Intervall beträgt: 2 Stunden.

- Geben Sie je nach Auswahl ggf. den Termin an.
- Wählen Sie ggf. Zusatzoptionen (je nach Auftragsart verfügbar):

- **Auftrag nachholen, wenn die Zeit bereits abgelaufen ist**
  Es werden Aufträge durchgeführt, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, beispielsweise bei ausgeschaltetem Computer.
- **Auftrag zusätzlich bei Internet-Verbindung starten (DFÜ)**
  Zusätzlich zur festgelegten Häufigkeit wird der Auftrag bei jedem Zustandekommen einer Internet-Verbindung durchgeführt.

- Klicken Sie auf **Weiter**.
  ↳ Das Dialogfenster **Auswahl des Darstellungsmodus** erscheint.
- Wählen Sie den Darstellungsmodus des Auftragsfensters:

- **Unsichtbar**: kein Auftragsfenster
- **Minimiert**: nur Fortschrittsbalken
- **Maximiert**: gesamtes Auftragsfenster

- Klicken Sie auf **Fertig stellen**.
  ↳ Ihr neu angelegter Auftrag erscheint auf der Startseite der Rubrik *VERWALTUNG* **> Planer** als aktiviert (Häkchen).
- Deaktivieren Sie ggf. die Aufträge, die nicht ausgeführt werden sollen.

Über folgende Symbole können Sie Aufträge weiter bearbeiten:

i Eigenschaften eines Auftrags ansehen

Auftrag ändern

Auftrag löschen

Auftrag starten

Auftrag stoppen

4.3.4 Ein Update manuell starten

Sie haben verschiedene Möglichkeiten ein Update manuell zu starten: Beim manuell gestarteten Update wird immer ein Update der Virendefinitionsdatei und der Suchengine durchgeführt.

So starten Sie manuell ein Update Ihres Avira Produkts:

- Klicken Sie mit der rechten Maustaste auf das Avira Tray Icon in der Taskleiste und wählen Sie **Update starten**.

  \- ODER -

- Wählen Sie im Control Center die Rubrik **Status**, dann klicken Sie im Bereich **Letztes Update** auf den Link **Update starten**.

  \- ODER -

  Wählen Sie im Control Center im Menü **Update** den Menübefehl **Update starten**.

  ↳ Das Dialogfenster **Updater** erscheint.

> **Hinweis**
> Wir empfehlen, regelmäßige automatische Updates durchzuführen. Das empfohlene Update-Intervall beträgt: 2 Stunden.

> **Hinweis**
> Sie können ein manuelles Update auch direkt über das Windows Sicherheitscenter ausführen.

4.3.5 Direktsuche: Mit einem Suchprofil nach Viren und Malware suchen

Ein Suchprofil ist eine Zusammenstellung von Laufwerken und Verzeichnissen, die durchsucht werden sollen.

Sie haben folgende Möglichkeit über ein Suchprofil zu suchen:

- Vordefiniertes Suchprofil verwenden

  Wenn die vordefinierten Suchprofile Ihren Bedürfnissen entsprechen.
- Suchprofil anpassen und verwenden (manuelle Auswahl)

  Wenn Sie mit einem individualisierten Suchprofil suchen möchten.
- Neues Suchprofil erstellen und verwenden

  Wenn Sie ein eigenes Suchprofil anlegen möchten.

Je nach Betriebssystem stehen für das Starten eines Suchprofils verschiedene Symbole zur Verfügung:

- Unter Windows XP:

   Mit diesem Symbol starten Sie die Suche über ein Suchprofil.

- Ab Windows Vista:

  Ab Microsoft Windows Vista hat das Control Center zunächst nur eingeschränkte Rechte z.B. für den Zugriff auf Verzeichnisse und Dateien. Bestimmte Aktionen und Dateizugriffe kann das Control Center nur mit erweiterten Administratorrechten ausführen. Diese erweiterten Administratorrechte müssen bei jedem Start einer Suche über ein Suchprofil erteilt werden.

  Mit diesem Symbol starten Sie eine eingeschränkte Suche über ein Suchprofil. Es werden nur die Verzeichnisse und Dateien durchsucht, für die das Betriebssystem die Zugriffsrechte erteilt hat.

  Mit diesem Symbol starten Sie die Suche mit erweiterten Administratorrechten. Nach einer Bestätigung werden alle Verzeichnisse und Dateien im gewählten Suchprofil durchsucht.

So suchen Sie mit einem Suchprofil nach Viren und Malware:

- Wählen Sie im Control Center die Rubrik *PC SICHERHEIT* **> System-Scanner**.

  ↳ Vordefinierte Suchprofile erscheinen.

- Wählen Sie eines der vordefinierten Suchprofile aus.

  -ODER-

  Passen Sie das Suchprofil **Manuelle Auswahl** an.

  -ODER-

  Erstellen Sie ein neues Suchprofil

- Klicken auf das Symbol (Windows XP: oder ab Windows Vista:).
- Das Fenster **Luke Filewalker** erscheint und die Direktsuche startet.

  ↳ Nach Ablauf des Suchprozesses werden die Ergebnisse angezeigt.

Wenn Sie ein Suchprofil anpassen möchten:

- Klappen Sie im Suchprofil **Manuelle Auswahl** den Dateibaum so weit auf, dass alle Laufwerke und Verzeichnisse geöffnet sind, die geprüft werden sollen

- Klick auf das **+** Zeichen: Nächste Verzeichnisebene wird angezeigt.
- Klick auf das **-** Zeichen: Nächste Verzeichnisebene wird verborgen.

- Markieren Sie die Knoten und Verzeichnisse, die geprüft werden sollen, durch einen Klick in das jeweilige Kästchen der jeweiligen Verzeichnisebene

  Sie haben folgende Möglichkeiten, Verzeichnisse auszuwählen:

- Verzeichnis einschließlich Unterverzeichnisse (schwarzes Häkchen)

- Nur Unterverzeichnisse in einem Verzeichnis (graues Häkchen, Unterverzeichnisse haben schwarze Häkchen)
- Kein Verzeichnis (kein Häkchen)

Wenn Sie ein neues Suchprofil erstellen möchten:

- Klicken Sie auf das Symbol **Neues Profil erstellen.**
  - ↳ Das Profil *Neues Profil* erscheint unterhalb der bisher vorhandenen Profile.
- Benennen Sie das Suchprofil ggf. um, indem Sie auf das Symbol klicken.
- Markieren Sie die Knoten und Verzeichnisse, die geprüft werden sollen, durch einen Klick in das Kästchen der jeweiligen Verzeichnisebene.

  Sie haben folgende Möglichkeiten, Verzeichnisse auszuwählen:

- Verzeichnis einschließlich Unterverzeichnisse (schwarzes Häkchen)
- Nur Unterverzeichnisse in einem Verzeichnis (graues Häkchen, Unterverzeichnisse haben schwarze Häkchen)
- Keine Verzeichnisse (kein Häkchen)

4.3.6 Direktsuche: Per Drag & Drop nach Viren und Malware suchen

So suchen Sie per Drag & Drop gezielt nach Viren und Malware:

- ✓ Das Control Center Ihres Avira Programms ist geöffnet.
- Markieren Sie die Datei oder das Verzeichnis, die/das geprüft werden soll.
- Ziehen Sie mit der linken Maustaste die markierte Datei oder das markierte Verzeichnis in das Control Center.
  - ↳ Das Fenster **Luke Filewalker** erscheint und die Direktsuche startet.
  - ↳ Nach Ablauf des Suchprozesses werden die Ergebnisse angezeigt.

4.3.7 Direktsuche: Über das Kontextmenü nach Viren und Malware suchen

So suchen Sie über das Kontextmenü gezielt nach Viren und Malware:

- Klicken Sie (z.B. im Windows Explorer, auf dem Desktop oder in einem geöffneten Windows-Verzeichnis) mit der rechten Maustaste auf die Datei bzw. das Verzeichnis, die/das Sie prüfen wollen.
  - ↳ Das Kontextmenü des Windows Explorers erscheint.
- Wählen Sie im Kontextmenü **Ausgewählte Dateien mit Avira überprüfen**.
  - ↳ Das Fenster **Luke Filewalker** erscheint und die Direktsuche startet.
  - ↳ Nach Ablauf des Suchprozesses werden die Ergebnisse angezeigt.

4.3.8 Direktsuche: Automatisiert nach Viren und Malware suchen

> **Hinweis**
> Nach der Installation ist der Prüfauftrag *Vollständige Systemprüfung* im Planer angelegt: In einem empfohlenen Intervall wird automatisch eine vollständige Systemprüfung ausgeführt.

So legen Sie einen Auftrag an, der automatisiert nach Viren und Malware sucht:

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* **> Planer**.
- Klicken Sie auf das Symbol [+] **Neuen Auftrag mit dem Wizard erstellen**.
  - ↳ Das Dialogfenster **Name und Beschreibung des Auftrags** erscheint.
- Benennen Sie den Auftrag und beschreiben Sie ihn gegebenenfalls.
- Klicken Sie auf **Weiter**.
  - ↳ Das Dialogfenster **Art des Auftrags** erscheint.
- Wählen Sie den **Prüfauftrag**.
- Klicken Sie auf **Weiter**.
  - ↳ Das Dialogfenster **Auswahl des Profils** erscheint.
- Wählen Sie, welches Profil durchsucht werden soll.
- Klicken Sie auf **Weiter**.
  - ↳ Das Dialogfenster **Zeitpunkt des Auftrags** erscheint.
- Wählen Sie aus, wann der Suchlauf ausgeführt werden soll:

- **Sofort**
- **Täglich**
- **Wöchentlich**
- **Intervall**
- **Einmalig**
- **Login**

- Geben Sie je nach Auswahl ggf. den Termin an.
- Wählen Sie ggf. folgende Zusatzoption (je nach Auftragsart verfügbar): **Auftrag nachholen, wenn die Zeit bereits abgelaufen ist**
  - ↳ Es werden Aufträge durchgeführt, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, beispielsweise bei ausgeschaltetem Computer.
- Klicken Sie auf **Weiter**.
  - ↳ Das Dialogfenster **Auswahl des Darstellungsmodus** erscheint.
- Wählen Sie den Darstellungsmodus des Auftragsfensters:

- **Unsichtbar**: kein Auftragsfenster
- **Minimiert**: nur Fortschrittsbalken
- **Maximiert**: gesamtes Auftragsfenster

- Wählen Sie die Option **Computer herunterfahren, wenn der Auftrag ausgeführt wurde**, wenn Sie möchten, dass der Rechner automatisch heruntergefahren wird, sobald der Auftrag ausgeführt und beendet wurde.

  Die Option ist nur im minimierten oder maximierten Darstellungsmodus verfügbar.

- Klicken Sie auf **Fertig stellen**.

  ↳ Ihr neu angelegter Auftrag erscheint auf der Startseite der Rubrik *VERWALTUNG* **> Planer** als aktiviert (Häkchen).

- Deaktivieren Sie ggf. die Aufträge, die nicht ausgeführt werden sollen.

Über folgende Symbole können Sie Aufträge weiter bearbeiten:

Eigenschaften zu einem Auftrag ansehen

Auftrag ändern

Auftrag löschen

Auftrag starten

Auftrag stoppen

4.3.9 Direktsuche: Gezielt nach aktiven Rootkits suchen

Um nach aktiven Rootkits zu suchen, nutzen Sie das vordefinierte Suchprofil **Suche nach Rootkits und aktiver Malware**.

So suchen Sie gezielt nach aktiven Rootkits:

- Wählen Sie im Control Center die Rubrik *PC SICHERHEIT* **> System-Scanner**.

  ↳ Vordefinierte Suchprofile erscheinen.

- Wählen Sie das vordefinierte Suchprofil **Suche nach Rootkits und aktiver Malware**.

- Markieren Sie ggf. weitere Knoten und Verzeichnisse, die geprüft werden sollen, durch einen Klick in das Kästchen der Verzeichnisebene.

- Klicken Sie auf das Symbol (Windows XP: oder ab Windows Vista:).

  ↳ Das Fenster **Luke Filewalker** erscheint und die Direktsuche startet.



↳ Nach Ablauf des Suchprozesses werden die Ergebnisse angezeigt.

4.3.10 Auf gefundene Viren und Malware reagieren

Für die einzelnen Schutzkomponenten Ihres Avira Produkts können Sie in der Konfiguration jeweils unter der Rubrik **Aktion bei Fund** einstellen, wie Ihr Avira Produkt bei einem Fund eines Virus oder unerwünschten Programms reagiert.

Bei der ProActiv-Komponente des Echtzeit-Scanners bestehen keine konfigurierbaren Aktionsoptionen: Ein Fund wird immer im Fenster **Echtzeit-Scanner: Verdächtiges Verhalten einer Anwendung** gemeldet.

Aktionsoptionen beim System-Scanner:

- **Interaktiv**

  Im interaktiven Aktionsmodus werden Funde der Suche des System-Scanners in einem Dialogfenster gemeldet. Diese Einstellung ist standardmäßig aktiviert.
  Bei der **Suche des System-Scanners** erhalten Sie beim Abschluss der Suche eine Warnmeldung mit einer Liste der gefundenen betroffenen Dateien. Sie haben die Möglichkeit, über das Kontextmenü eine auszuführende Aktion für die einzelnen betroffenen Dateien auszuwählen. Sie können die gewählten Aktionen für alle betroffenen Dateien ausführen oder den System-Scanner beenden.

- **Automatisch**

  Im automatischen Aktionsmodus wird bei einem Fund eines Virus oder unerwünschten Programms automatisch die Aktion ausgeführt, die Sie in diesem Bereich ausgewählt haben.

Aktionsoptionen beim Echtzeit-Scanner:

- **Interaktiv**

  Im interaktiven Aktionsmodus wird der Datenzugriff verweigert und eine Desktop-Benachrichtigung angezeigt. In der Desktop-Benachrichtigung können Sie die gefundene Malware entfernen oder über die Schaltfläche **Details** zur weiteren Virenbehandlung an die Komponente System-Scanner übergeben. Der System-Scanner meldet den Fund in einem Fenster, in dem Sie über ein Kontextmenü verschiedene Optionen zur Behandlung der betroffenen Datei haben (siehe Fund > System-Scanner).

- **Automatisch**

  Im automatischen Aktionsmodus wird beim Fund eines Virus oder unerwünschten Programms automatisch die Aktion ausgeführt, die Sie in diesem Bereich ausgewählt haben.

Aktionsoptionen beim Email-Schutz, Browser-Schutz:

- **Interaktiv**

  Im interaktiven Aktionsmodus erscheint bei einem Fund eines Virus bzw. unerwünschten Programms ein Dialogfenster, in dem Sie auswählen können, was

mit dem betroffenen Objekt weiter geschehen soll. Diese Einstellung ist standardmäßig aktiviert.

- **Automatisch**

  Im automatischen Aktionsmodus wird bei einem Fund eines Virus oder unerwünschten Programms automatisch die Aktion ausgeführt, die Sie in diesem Bereich ausgewählt haben.

Interaktiver Aktionsmodus

- Im interaktiven Aktionsmodus reagieren Sie auf gefundene Viren und unerwünschte Programme, indem Sie in der Warnmeldung eine **Aktion für die betroffenen Objekte** auswählen und die gewählte Aktion durch **Bestätigen** ausführen.

Folgende Aktionen zur Behandlung betroffener Objekte stehen zur Auswahl:

> **Hinweis**
> Welche Aktionen zur Auswahl stehen, ist abhängig vom Betriebssystem, von der Schutzkomponente (Avira System-Scanner, Avira Echtzeit-Scanner, Avira Email-Schutz, Avira Browser-Schutz), die den Fund meldet und von der gefundenen Malware.

Aktionen des System-Scanners und des Echtzeit-Scanners (ohne Funde von ProActiv):

- **Reparieren**

  Die Datei wird repariert.
  Diese Option ist nur aktivierbar, wenn eine Reparatur der gefundenen Datei möglich ist.

- **Umbenennen**

  Die Datei wird nach **.vir* umbenannt. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurückbenannt werden.

- **Quarantäne**

  Die Datei wird in ein spezielles Format (**.qua*) gepackt und in das Quarantäne-Verzeichnis *INFECTED* auf Ihrer Festplatte verschoben, sodass kein direkter Zugriff mehr möglich ist. Dateien in diesem Verzeichnis können später in der Quarantäne repariert oder - falls nötig - an Avira geschickt werden.

- **Löschen**

  Die Datei wird gelöscht. Dieser Vorgang ist bedeutend schneller als **Überschreiben und löschen**.
  Handelt es sich bei dem Fund um einen Bootsektorvirus, wird beim Löschen der Bootsektor gelöscht. Es wird ein neuer Bootsektor geschrieben.

- **Ignorieren**

  Es werden keine weiteren Aktionen ausgeführt. Die betroffene Datei bleibt auf Ihrem Computer aktiv.

- **Überschreiben und löschen**

  Die Datei wird mit einem Standardmuster überschrieben und anschließend gelöscht. Sie kann nicht wiederhergestellt werden.

> **Warnung**
> Gefahr von Datenverlust und Schäden am Betriebssystem!
> Nutzen Sie die Option **Ignorieren** nur in begründeten Ausnahmefällen.

- **Immer ignorieren**

  Aktionsoption bei Funden des Echtzeit-Scanners: Es werden keine weiteren Aktionen vom Echtzeit-Scanner ausgeführt. Ein Zugriff auf die Datei wird zugelassen. Alle weiteren Zugriffe auf diese Datei werden zugelassen und nicht mehr gemeldet bis ein Neustart des Rechners oder ein Update der Virendefinitionsdatei erfolgt.

- **In Quarantäne kopieren**

  Aktionsoption beim Fund eines Rootkits: Der Fund wird in die Quarantäne kopiert.

- **Bootsektor reparieren | Repairtool herunterladen**

  Aktionsoptionen beim Fund von infizierten Bootsektoren: Für infizierte Diskettenlaufwerke stehen Optionen zur Reparatur zur Verfügung. Ist keine Reparatur mit Ihrem Avira Produkt möglich, können Sie ein Spezialtool zum Erkennen und Entfernen von Bootsektorviren herunterladen.

> **Hinweis**
> Wenn Sie Aktionen auf laufende Prozesse anwenden, werden die betroffenen Prozesse vor der Ausführung der Aktion beendet.

Aktionen des Echtzeit-Scanners bei Funden der ProActiv-Komponente (Meldung von verdächtigen Aktionen einer Anwendung):

- **Vertrauenswürdiges Programm**

  Die Ausführung der Anwendung wird fortgesetzt. Das Programm wird zur Liste der erlaubten Anwendungen hinzugefügt und von der Überwachung durch die ProActiv-Komponente ausgenommen. Beim Hinzufügen zur Liste der erlaubten Anwendungen wird der Überwachungstyp *Inhalt* gesetzt. Dies bedeutet, dass die Anwendung nur bei unverändertem Inhalt von einer Überwachung durch die ProActiv-Komponente ausgenommen wird (siehe Anwendungsfilter: Auszulassende Anwendungen).

- **Programm einmal blockieren**

  Die Anwendung wird blockiert, d.h. die Ausführung der Anwendung wird beendet. Die Aktionen der Anwendung werden weiterhin von der ProActiv-Komponente überwacht.



- **Dieses Programm immer blockieren**

  Die Anwendung wird blockiert, d.h. die Ausführung der Anwendung wird beendet. Das Programm wird zur Liste der zu blockierenden Anwendungen hinzugefügt und kann nicht mehr ausgeführt werden (siehe Anwendungsfilter: Zu blockierende Anwendungen).

- **Ignorieren**

  Die Ausführung der Anwendung wird fortgesetzt. Die Aktionen der Anwendung werden weiterhin von der ProActiv-Komponente überwacht.

Aktionen des Email-Schutzes: Eingehende Emails

- **In Quarantäne verschieben**

  Die Email wird inklusive aller Anhänge in Quarantäne verschoben. Die betroffene Email wird gelöscht. Textkörper und ggf. Anhänge der Email werden durch einen Standardtext ersetzt.

- **Mail löschen**

  Die betroffene Email wird gelöscht. Textkörper und ggf. Anhänge werden durch einen Standardtext ersetzt.

- **Anhang löschen**

  Der betroffene Anhang wird durch einen Standardtext ersetzt. Sollte der Textkörper der Email betroffen sein, wird dieser gelöscht und ebenfalls durch einen Standardtext ersetzt. Die Email selbst wird zugestellt.

- **Anhang in Quarantäne verschieben**

  Der betroffene Anhang wird in Quarantäne gestellt und anschließend gelöscht (durch einen Standardtext ersetzt). Der Textkörper der Email wird zugestellt. Die betroffene Anlage kann später über den Quarantänemanager zugestellt werden.

- **Ignorieren**

  Die betroffene Email wird zugestellt.

> **Warnung**
> Hierdurch können Viren sowie unerwünschte Programme auf Ihr Computersystem gelangen. Wählen Sie die Option **Ignorieren** nur in begründeten Ausnahmefällen. Deaktivieren Sie die Vorschau in Microsoft Outlook, starten Sie Anlagen auf keinen Fall per Doppelklick!

Aktionen des Email-Schutzes: Ausgehende Emails

- **Mail in Quarantäne verschieben (nicht senden)**

  Die Email wird inklusive aller Anhänge in die Quarantäne kopiert und nicht gesendet. Die Email verbleibt im Postausgang Ihres Email-Client. Sie erhalten in Ihrem Email-Programm eine Fehlermeldung. Bei jedem weiteren Sendevorgang Ihres Email-Kontos wird diese Email auf Malware geprüft.

- **Mailversand blockieren (nicht senden)**

Die Email wird nicht versandt und verbleibt im Postausgang Ihres Email-Client. Sie erhalten in Ihrem Email-Programm eine Fehlermeldung. Bei jedem weiteren Sendevorgang Ihres Email-Kontos wird diese Email auf Malware geprüft.

- **Ignorieren**

  Die betroffene Email wird versendet.

> **Warnung**
> Hierdurch können Viren sowie unerwünschte Programme auf das Computersystem des Email-Empfängers gelangen.

Aktionen des Browser-Schutzes:

- **Zugriff verweigern**

  Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden nicht an Ihren Webbrowser gesendet. Im Webbrowser wird eine Fehlermeldung zur Zugriffsverweigerung angezeigt.

- **Quarantäne**

  Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden in die Quarantäne verschoben. Die betroffene Datei kann vom Quarantänemanager aus wiederhergestellt werden, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden.

- **Ignorieren**

  Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden vom Browser-Schutz an Ihren Webbrowser weitergeleitet.

> **Warnung**
> Hierdurch können Viren sowie unerwünschte Programme auf Ihr Computersystem gelangen. Wählen Sie die Option **Ignorieren** nur in begründeten Ausnahmefällen.

> **Hinweis**
> Wir empfehlen, eine verdächtige Datei, die nicht repariert werden kann, in die Quarantäne zu verschieben.

> **Hinweis**
> Schicken Sie uns auch Dateien, die von der Heuristik gemeldet werden, zur Analyse zu.
> Sie können diese Dateien z.B. über unsere Webseite hochladen:
> http://www.avira.de/sample-upload



Dateien, die von der Heuristik gemeldet werden, erkennen Sie an der Bezeichnung *HEUR/* bzw. *HEURISTIC/*, die dem Dateinamen vorangestellt werden, z.B.: *HEUR/testdatei.**.

4.3.11 Quarantäne: Mit Dateien (*.qua) in Quarantäne umgehen

So können Sie mit Dateien in der Quarantäne umgehen:

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* **> Quarantäne**.
- Prüfen Sie, um welche Dateien es sich handelt, sodass Sie deren Originale ggf. von anderer Stelle zurück auf Ihren Computer laden können.

Wenn Sie nähere Informationen zu einer Datei ansehen wollen:

- Markieren Sie die Datei und klicken Sie auf [i].
  - ↳ Das Dialogfenster **Eigenschaften** mit weiteren Informationen zur Datei erscheint.

Wenn Sie eine Datei erneut prüfen wollen:

Die Prüfung einer Datei empfiehlt sich, wenn die Virendefinitionsdatei Ihres Avira Produkts aktualisiert wurde und ein Verdacht auf einen Fehlalarm vorliegt. So können Sie einen Fehlalarm beim erneuten Prüfen bestätigen und die Datei wiederherstellen.

- Markieren Sie die Datei und klicken Sie auf [Lupe].
  - ↳ Die Datei wird mit den Einstellungen der Direktsuche auf Viren und Malware geprüft.
  - ↳ Nach der Prüfung erscheint der Dialog **Prüfstatistik**, der eine Statistik zum Zustand der Datei vor und nach der erneuten Prüfung anzeigt.

Wenn Sie eine Datei löschen wollen:

- Markieren Sie die Datei und klicken Sie auf [X].
- Sie müssen Ihre Auswahl mit **Ja** bestätigen.

Wenn Sie die Datei zur Analyse auf einen Webserver des Avira Malware Research Center hochladen möchten:

- Markieren Sie die Datei, die Sie hochladen möchten.
- Klicken Sie auf [Umschlag].
  - ↳ Es öffnet sich der Dialog *Datei-Upload* mit einem Formular zur Eingabe Ihrer Kontaktdaten.
- Geben Sie die Daten vollständig an.

- Wählen Sie einen Typ aus: **Verdächtige Datei** oder **Verdacht auf Fehlalarm**.
- Wählen Sie ein Antwortformat aus: **HTML**, **Text**, **HTML & Text**.
- Klicken Sie **OK.**
  - ↳ Die Datei wird gepackt auf einen Webserver des Avira Malware Research Center hochgeladen.

> **Hinweis**
> In folgenden Fällen wird eine Analyse durch das Avira Malware Research Center empfohlen:
> **Heuristischer Treffer (Verdächtige Datei)**: Bei einem Suchlauf wurde eine Datei von Ihrem Avira Produkt als verdächtig eingestuft und in die Quarantäne verschoben: Im Dialogfenster zum Virenfund oder in der Reportdatei des Suchlaufs wurde die Analyse der Datei durch das Avira Malware Research Center empfohlen.
> **Verdächtige Datei**: Sie halten eine Datei für verdächtig und haben diese deshalb zur Quarantäne hinzugefügt, die Prüfung der Datei auf Viren und Malware ist jedoch negativ.
> **Verdacht auf Fehlalarm**: Sie gehen davon aus, dass es sich bei einem Virenfund um einen Fehlalarm handelt: Ihr Avira Produkt meldet einen Fund in einer Datei die jedoch mit hoher Wahrscheinlichkeit nicht von Malware betroffen ist.

> **Hinweis**
> Die Größe der Dateien, die Sie hochladen, ist begrenzt auf 20 MB ungepackt oder 8 MB gepackt.

> **Hinweis**
> Sie können jeweils nur eine einzelne Datei hochladen.

Wenn Sie ein Quarantäne-Objekt aus der Quarantäne in ein anderes Verzeichnis kopieren möchten:

- Markieren Sie das Quarantäne-Objekt und klicken Sie auf  .
  - ↳ Es öffnet sich der Dialog *Ordner suchen*, in dem Sie ein Verzeichnis auswählen können.
- Wählen Sie ein Verzeichnis aus, in dem eine Kopie des Quarantäne-Objekts abgelegt werden soll und bestätigen Sie Ihre Auswahl mit **OK**.
  - ↳ Das ausgewählte Quarantäne-Objekt wird im ausgewählten Verzeichnis abgelegt.

> **Hinweis**
> Das Quarantäne-Objekt ist nicht identisch mit der wiederhergestellten Datei. Das Quarantäne-Objekt ist verschlüsselt und kann nicht ausgeführt oder im Ursprungsformat gelesen werden.

Wenn Sie die Eigenschaften eines Quarantäne-Objekts in eine Textdatei exportieren möchten:

- Markieren Sie das Quarantäne-Objekt und klicken Sie auf  .
  - ↳ Es öffnet sich eine Textdatei mit den Daten zum ausgewählten Quarantäne-Objekt.
- Speichern Sie die Textdatei ab.

Dateien in Quarantäne können Sie auch wiederherstellen (siehe Kapitel: Quarantäne: Dateien in der Quarantäne wiederherstellen).

4.3.12 Quarantäne: Dateien in der Quarantäne wiederherstellen

Je nach Betriebsystem stehen für das Wiederherstellen verschiedene Symbole zur Verfügung:

- **Unter Windows XP und 2000**:

  Mit diesem Symbol stellen Sie Dateien im ursprünglichen Verzeichnis wieder her.

  Mit diesem Symbol stellen Sie Dateien in einem Verzeichnis Ihrer Wahl wieder her.

- **Ab Windows Vista**:

  Ab Microsoft Windows Vista hat das Control Center zunächst nur eingeschränkte Rechte z.B. für den Zugriff auf Verzeichnisse und Dateien. Bestimmte Aktionen und Dateizugriffe kann das Control Center nur mit erweiterten Administratorrechten ausführen. Diese erweiterten Administratorrechte müssen bei jedem Start einer Suche über ein Suchprofil erteilt werden.

  Mit diesem Symbol stellen Sie Dateien in einem Verzeichnis Ihrer Wahl wieder her.

  Mit diesem Symbol stellen Sie Dateien im ursprünglichen Verzeichnis wieder her. Wenn für den Zugriff auf dieses Verzeichnis erweiterte Administratorrechte nötig sind, erscheint eine entsprechende Abfrage.

So können Sie Dateien in der Quarantäne wiederherstellen:

Warnung
Gefahr von Datenverlust und Schäden am Betriebssystem des Computers! Verwenden Sie die Funktion **Ausgewähltes Objekt wiederherstellen** nur in Ausnahmefällen. Stellen Sie nur solche Dateien wieder her, die durch einen erneuten Suchlauf repariert werden konnten.

✓ Datei erneut mit Suchlauf geprüft und repariert.

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* **> Quarantäne**.

Hinweis

Emails und Anhänge von Emails können nur mit der Option und mit der Endung **.eml* wiederhergestellt werden.

Wenn Sie eine Datei an ihrem Ursprungsort wiederherstellen wollen:

- Markieren Sie die Datei und klicken Sie auf das Symbol (Windows XP: , ab Windows Vista).

Diese Option ist für Emails nicht möglich.

Hinweis

Emails und Anhänge von Emails können nur mit der Option und mit der Endung **.eml* wiederhergestellt werden.

↳ Eine Abfrage erscheint, ob Sie die Datei wiederherstellen wollen.

- Klicken Sie auf **Ja**.

↳ Die Datei wird in dem Verzeichnis wiederhergestellt, aus dem sie in die Quarantäne verschoben wurde.

Wenn Sie eine Datei in einem bestimmten Verzeichnis wiederherstellen wollen:

- Markieren Sie die Datei und klicken Sie auf .

↳ Eine Abfrage erscheint, ob Sie die Datei wiederherstellen wollen.

- Klicken Sie auf **Ja**.

↳ Das Windows-Standardfenster für die Auswahl des Verzeichnisses erscheint.

- Wählen Sie das Verzeichnis, in dem die Datei wiederhergestellt werden soll und bestätigen Sie.

↳ Die Datei wird in dem gewählten Verzeichnis wiederhergestellt.



4.3.13 Quarantäne: Verdächtige Datei in die Quarantäne verschieben

So können Sie manuell eine verdächtige Datei in die Quarantäne verschieben:

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* **> Quarantäne**.
- Klicken Sie auf [+] .
  - ↳ Das Windows-Standardfenster für die Auswahl einer Datei erscheint.
- Wählen Sie die Datei und bestätigen Sie mit **Öffnen**.
  - ↳ Die Datei wird in die Quarantäne verschoben.

Dateien in Quarantäne können Sie mit dem Avira System-Scanner prüfen (siehe Kapitel: Quarantäne: Mit Dateien (*.qua) in Quarantäne umgehen).

4.3.14 Suchprofil: Dateityp in einem Suchprofil ergänzen oder löschen

So legen Sie für ein Suchprofil fest, dass zusätzliche Dateitypen durchsucht oder dass bestimmte Dateitypen von der Suche ausgeschlossen werden sollen (nur bei manueller Auswahl und selbstdefinierten Suchprofilen möglich):

- ✓ Sie befinden sich im Control Center in der Rubrik *PC SICHERHEIT* **> System Scanner**.
- Klicken Sie mit der rechten Maustaste auf das Suchprofil, das Sie bearbeiten wollen.
  - ↳ Ein Kontextmenü erscheint.
- Wählen Sie den Eintrag **Dateifilter**.
- Klappen Sie das Kontextmenü weiter auf, indem Sie auf das kleine Dreieck auf der rechten Seite des Kontextmenüs klicken.
  - ↳ Die Einträge **Standard**, **Prüfe alle Dateien** und **Benutzerdefiniert** erscheinen.
- Wählen Sie den Eintrag **Benutzerdefiniert**.
  - ↳ Das Dialogfenster **Dateierweiterungen** erscheint mit einer Liste aller Dateitypen, die mit dem Suchprofil durchsucht werden.

Wenn Sie einen Dateityp aus der Suche ausschließen wollen:

- Markieren Sie den Dateityp und klicken Sie auf **Löschen**.

Wenn Sie einen Dateityp zur Suche hinzufügen wollen:

- Markieren Sie einen Dateityp.
- Klicken Sie auf **Einfügen** und geben Sie die Dateierweiterung des Dateityps in das Eingabefeld ein.

  Verwenden Sie dabei maximal 10 Zeichen und geben Sie den führenden Punkt nicht mit an. Platzhalter (* und ?) sind erlaubt.

4.3.15 Suchprofil: Desktop-Verknüpfung für Suchprofil erstellen

Über eine Desktop-Verknüpfung zu einem Suchprofil können Sie eine Direktsuche direkt von Ihrem Desktop aus starten, ohne das Control Center Ihres Avira Produktes aufzurufen.

So erstellen Sie eine Verknüpfung zu dem Suchprofil auf dem Desktop:

✓ Sie befinden sich im Control Center in der Rubrik *PC SICHERHEIT* **> System Scanner**.

- Wählen Sie das Suchprofil, zu dem Sie eine Verknüpfung erstellen möchten.
- Klicken Sie auf das Symbol .
  - ↳ Die Desktop-Verknüpfung wird erstellt.

4.3.16 Ereignisse: Ereignisse filtern

Im Control Center werden unter *VERWALTUNG* **> Ereignisse** alle Ereignisse angezeigt, die von den Programmkomponenten Ihres Avira Produkts erzeugt wurden (analog der Ereignisanzeige Ihres Windows Betriebssystems). Die Programmkomponenten, in ihrer alphabetischen Reihenfolge, sind die folgenden:

- Backup
- Browser-Schutz
- Echtzeit-Scanner
- Email-Schutz
- FireWall
- Hilfsdienst
- Planer
- Sicher Surfen
- System-Scanner
- Updater

Es werden folgende Ereignistypen angezeigt:

- *Information*
- *Warnung*
- *Fehler*
- *Fund*

So filtern Sie die angezeigten Ereignisse:

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* **> Ereignisse**.

- Aktivieren Sie die Kontrollkästchen der Programmkomponenten, um die Ereignisse der aktivierten Komponenten anzuzeigen.

  - ODER -

  Deaktivieren Sie die Kontrollkästchen der Programmkomponenten, um die Ereignisse der deaktivierten Komponenten auszublenden.

- Aktivieren Sie die Kontrollkästchen der Ereignistypen, um diese Ereignisse anzuzeigen.

  - ODER -

  Deaktivieren Sie die Kontrollkästchen der Ereignistypen, um diese Ereignisse auszublenden.

4.3.17 Email-Schutz: Email-Adressen von der Prüfung ausschließen

So stellen Sie ein, welche Email-Adressen (Absender) von der Prüfung durch den Email-Schutz ausgeschlossen werden (sogenanntes Whitelisting):

- Wählen Sie im Control Center die Rubrik *INTERNET SICHERHEIT* **> Email-Schutz**.

  ↳ In der Liste sehen Sie die eingegangenen Emails.

- Markieren Sie die Email, die Sie von der Prüfung des Email-Schutzes ausschließen möchten.

- Klicken Sie auf das gewünschte Symbol, um die Email von der Prüfung des Email-Schutzes auszuschließen:

  Die ausgewählte Email-Adresse wird in Zukunft nicht mehr auf Viren und unerwünschte Programme geprüft.

  Die ausgewählte Email-Adresse wird in Zukunft nicht mehr auf Spam geprüft.

  ↳ Die Email-Absender-Adresse wird in die Ausschlussliste übernommen und nicht mehr auf Viren und Malware oder Spam geprüft.

Warnung
Schließen Sie nur Email-Adressen von absolut vertrauenswürdigen Absendern von der Prüfung des Email-Schutz aus.

Hinweis
In der Konfiguration unter Email-Schutz > Allgemeines > Ausnahmen können Sie weitere Email-Adressen in die Ausschlussliste einpflegen oder Email-Adressen aus der Ausschlussliste entfernen.



4.3.18 Email-Schutz: Das AntiSpam Modul trainieren

Das AntiSpam Modul enthält eine Trainingsdatenbank. In diese Trainingsdatenbank werden Ihre individuellen Kategorisierungskriterien aufgenommen. Im Lauf der Zeit stellen sich so die internen Filter, Algorithmen und Bewertungskriterien für Spam auf Ihre persönlichen Kriterien ein.

So kategorisieren Sie Emails für die Trainingsdatenbank:

- Wählen Sie im Control Center die Rubrik *INTERNET SICHERHEIT* **> Email-Schutz**.
  - ↳ In der Liste sehen Sie die eingehenden Emails.
- Markieren Sie die Email, die Sie kategorisieren möchten.
- Klicken Sie auf das gewünschte Symbol, um die Email z.B. als *Spam* oder als erwünschte (*'gute'*) Email zu kennzeichnen.
  - ↳ Die Email wird in die Trainingsdatenbank übernommen und beim nächsten Mal zur Spam-Erkennung genutzt.

> **Hinweis**
> Sie können die Trainingsdatenbank in der Konfiguration unter **Email-Schutz > Allgemeines > AntiSpam** löschen.
>
> **Hinweis**
> Der Ausschluss einzelner Email-Adressen von der Prüfung auf Malware bezieht sich natürlich nur auf eingehende Emails. Die AntiSpam-Trainingsfunktionen und AntiSpam-Ausnahmen beziehen sich ebenso ausschließlich auf eingehende Emails. Um die Prüfung ausgehender Emails abzuschalten, deaktivieren Sie die Prüfung ausgehender Emails in der Konfiguration unter Email-Schutz > Suche.

4.3.19 FireWall: Sicherheitsstufe für die FireWall wählen

Sie können zwischen verschiedenen Sicherheitsstufen wählen. Abhängig davon haben Sie unterschiedliche Konfigurationsmöglichkeiten für die Adapterregeln.

Folgende Sicherheitsniveaus stehen zur Verfügung:

- **Niedrig**

  Flooding und Port-Scan werden erkannt.
- **Mittel**

  Verdächtige TCP- und UDP-Pakete werden verworfen.
  Flooding und Port-Scan werden verhindert.
  (Standard-Einstellung)



- **Hoch**

  Der Computer ist im Netzwerk unsichtbar.
  Neue Verbindungen von außen sind nicht erlaubt.
  Flooding und Port-Scan werden verhindert.

- **Benutzer**

  Benutzerdefinierte Regeln: Auf dieses Sicherheitsniveau stellt das Programm automatisch um, wenn Sie Adapterregeln geändert haben.

- **Alle blockieren**

  Beendet alle bestehenden Netzwerkverbindungen.

> **Hinweis**
> Die Standardeinstellung des Sicherheitsniveaus für alle vordefinierten Regeln der Avira FireWall ist **Mittel.**

So stellen Sie das Sicherheitsniveau für die FireWall ein:

- Wählen Sie im Control Center die Rubrik *INTERNET SICHERHEIT* **> FireWall**.
- Stellen Sie den Schieberegler auf das gewünschte Sicherheitsniveau.
  - ↳ Das gewählte Sicherheitsniveau ist sofort aktiv.

4.3.20 Backup: Backups manuell erstellen

Über das Backup-Tool im Control Center können Sie schnell und einfach eine Sicherung Ihrer persönlichen Daten erstellen. Mit Avira Backup erstellen Sie sog. Spiegel-Backups, mit denen Sie ressourcenschonend jeweils den aktuellsten Stand Ihrer Daten sichern und vorhalten können. Beim Sichern mit Avira Backup können die zu sichernden Daten auf Viren und Malware geprüft werden. Betroffene Dateien werden nicht gesichert.

> **Hinweis**
> Beim Spiegel-Backup werden im Unterschied zum Versions-Backup keine einzelnen Backup-Versionen vorgehalten. Das Spiegel-Backup enthält den Datenbestand zum Zeitpunkt des letzten Backups. Werden Dateien jedoch aus dem zu sichernden Datenbestand gelöscht, findet kein Abgleich beim folgenden Backup statt, d.h. die gelöschten Dateien befinden sich noch im Backup.

> **Hinweis**
> Beim Avira Backup mit Standardeinstellungen werden nur geänderte Dateien gesichert, und es erfolgt eine Prüfung auf Viren und Malware. Sie können diese Einstellungen in der Konfiguration unter Backup > Einstellungen ändern.

So sichern Sie mit dem Backup-Tool Ihre Daten:



- Wählen Sie im Control Center die Rubrik *PC SICHERHEIT* **> Backup**.
  - ↳ Vordefinierte Backup-Profile erscheinen.
- Wählen Sie eines der vordefinierten Backup-Profile aus.

  -ODER-

  Passen Sie das Backup-Profil **Manuelle Auswahl** an.

  -ODER-

  Erstellen Sie ein neues Backup-Profil
- Geben Sie für das gewählte Profil im Feld **Zielverzeichnis** einen Sicherungsort an.

  Sie können als Sicherungsort für das Backup ein Verzeichnis auf Ihrem Rechner oder auf einem verbundenen Netzlaufwerk sowie einen Wechseldatenträger wie USB-Stick oder Diskette angeben.
- Klicken auf das Symbol .
  - ↳ Das Fenster **Avira Backup** erscheint und das Backup startet. Status und Ergebnisse des Backups werden im Backup-Fenster angezeigt.

Wenn Sie ein Backup-Profil anpassen möchten:

- Klappen Sie im Suchprofil **Manuelle Auswahl** den Dateibaum so weit auf, dass alle Laufwerke und Verzeichnisse geöffnet sind, die gesichert werden sollen:
- Klick auf das **+** Zeichen: Nächste Verzeichnisebene wird angezeigt.
- Klick auf das **-** Zeichen: Nächste Verzeichnisebene wird verborgen.
- Markieren Sie die Knoten und Verzeichnisse, die gesichert werden sollen, durch einen Klick in das jeweilige Kästchen der einzelnen Verzeichnisebene:

  Sie haben folgende Möglichkeiten, Verzeichnisse auszuwählen:
- Verzeichnis einschließlich Unterverzeichnisse (schwarzes Häkchen)
- Nur Unterverzeichnisse in einem Verzeichnis (graues Häkchen, Unterverzeichnisse haben schwarze Häkchen)
- Kein Verzeichnis (kein Häkchen)

Wenn Sie ein neues Backup-Profil erstellen möchten:

- Klicken Sie auf das Symbol **Neues Profil erstellen**.
  - ↳ Das Profil *Neues Profil* erscheint unterhalb der bisher vorhandenen Profile.
- Benennen Sie das Backup-Profil ggf. um, indem Sie auf das Symbol klicken.
- Markieren Sie die Knoten und Verzeichnisse, die gesichert werden sollen, durch einen Klick in das Kästchen der jeweiligen Verzeichnisebene.

  Sie haben folgende Möglichkeiten, Verzeichnisse auszuwählen:
- Verzeichnis einschließlich Unterverzeichnisse (schwarzes Häkchen)



- Nur Unterverzeichnisse in einem Verzeichnis (graues Häkchen, Unterverzeichnisse haben schwarze Häkchen)
- Keine Verzeichnisse (kein Häkchen)

4.3.21 Backup: Automatisiert Datensicherungen erstellen

So legen Sie einen Auftrag an, mit dem Sie automatisiert Datensicherungen erstellen:

- Wählen Sie im Control Center die Rubrik *VERWALTUNG* **> Planer**.
- Klicken Sie auf das Symbol [+] .
  - ↳ Das Dialogfenster **Name und Beschreibung des Auftrags** erscheint.
- Benennen Sie den Auftrag und beschreiben Sie ihn gegebenenfalls.
- Klicken Sie auf **Weiter**.
  - ↳ Das Dialogfenster **Art des Auftrags** erscheint.
- Wählen Sie den Eintrag **Backup-Auftrag**.
- Klicken Sie auf **Weiter**.
  - ↳ Das Dialogfenster **Auswahl des Profils** erscheint.
- Wählen Sie, welches Profil durchsucht werden soll.

> **Hinweis**
> Es werden ausschließlich Backup-Profile angezeigt, für die ein Sicherungsort angegeben wurde.

- Klicken Sie auf **Weiter**.
  - ↳ Das Dialogfenster **Zeitpunkt des Auftrags** erscheint.
- Wählen Sie aus, wann der Suchlauf ausgeführt werden soll:

- **Sofort**
- **Täglich**
- **Wöchentlich**
- **Intervall**
- **Einmalig**
- **Login**
- **Plug&Play**

  Beim Ereignis **Plug&Play** wird immer dann eine Sicherung erstellt, wenn der Wechseldatenträger, der für das Backup-Profil als Sicherungsort ausgewählt wurde, an den Computer angeschlossen wird. Das Backup-Ereignis **Plug&Play** setzt voraus, dass ein USB-Stick als Sicherungsort angegeben wurde.

- Geben Sie je nach Auswahl ggf. den Termin an.

- Wählen Sie ggf. folgende Zusatzoption (nur je nach Auftragsart verfügbar): **Auftrag nachholen, wenn die Zeit bereits abgelaufen ist**
  - ↳ Es werden Aufträge durchgeführt, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, beispielsweise bei ausgeschaltetem Computer.
- Klicken Sie auf **Weiter**.
  - ↳ Das Dialogfenster **Auswahl des Darstellungsmodus** erscheint.
- Wählen Sie den Darstellungsmodus des Auftragsfensters:

- **Minimiert**: nur Fortschrittsbalken
- **Maximiert**: gesamtes Backup-Fenster
- **Unsichtbar**: kein Backup-Fenster

- Klicken Sie auf **Fertig stellen**.
  - ↳ Ihr neu angelegter Auftrag erscheint auf der Startseite der Rubrik *VERWALTUNG* **> Planer** als aktiviert (Häkchen).
- Deaktivieren Sie ggf. die Aufträge, die nicht ausgeführt werden sollen.

Über folgende Symbole können Sie Aufträge weiter bearbeiten:

Eigenschaften zu einem Auftrag ansehen

Auftrag ändern

Auftrag löschen

Auftrag starten

Auftrag stoppen

5. System-Scanner

Mit der Komponente System-Scanner können Sie gezielte Suchläufe nach Viren und unerwünschten Programmen (Direktsuche) ausführen. Sie haben folgende Möglichkeiten nach betroffenen Dateien zu suchen:

- **Direktsuche über Kontextmenü**
  Die Direktsuche über das Kontextmenü (rechte Maustaste - Eintrag **Ausgewählte Dateien mit Avira überprüfen**) empfiehlt sich, wenn Sie z.B. im Windows Explorer einzelne Dateien und Verzeichnisse prüfen wollen. Ein weiterer Vorteil ist, dass für die Direktsuche über das Kontextmenü das Control Center nicht erst gestartet werden muss.
- **Direktsuche über Drag & Drop**
  Beim Ziehen einer Datei oder eines Verzeichnisses in das Programmfenster des Control Center prüft der System-Scanner die Datei bzw. das Verzeichnis sowie alle enthaltenen Unterverzeichnisse. Dieses Vorgehen empfiehlt sich, wenn Sie einzelne Dateien und Verzeichnisse prüfen wollen, die Sie z.B. auf Ihrem Desktop abgelegt haben.
- **Direktsuche über Profile**
  Dieses Vorgehen empfiehlt sich, wenn Sie regelmäßig bestimmte Verzeichnisse und Laufwerke (z.B. Ihr Arbeitsverzeichnis oder Laufwerke, auf denen Sie regelmäßig neue Dateien ablegen) prüfen wollen. Sie müssen diese Verzeichnisse und Laufwerke dann nicht für jede Prüfung neu wählen, sondern wählen eine Auswahl bequem mit dem entsprechenden Profil.
- **Direktsuche über den Planer**
  Der Planer bietet die Möglichkeit, zeitlich gesteuerte Prüfaufträge durchführen zu lassen.

Bei der Suche nach Rootkits, Bootsektorviren und beim Durchsuchen von aktiven Prozessen sind besondere Verfahren erforderlich. Sie haben folgende Optionen:

- Suche nach Rootkits über das Suchprofil **Suche nach Rootkits und aktiver Malware**
- Durchsuchen von aktiven Prozessen über das **Suchprofil Aktive Prozesse**
- Suche nach Bootsektorviren über den Menübefehl **Bootsektorviren prüfen...** im Menü **Extras**



6. Updates

Die Wirksamkeit einer Antivirensoftware steht und fällt mit der Aktualität des Programms, insbesondere der Virendefinitionsdatei und der Suchengine. Zur Ausführung von Updates ist die Komponente Updater in Ihr Avira Produkt integriert. Der Updater sorgt dafür, dass Ihr Avira Produkt stets auf dem neuesten Niveau arbeitet und in der Lage ist, die täglich neu erscheinenden Viren zu erfassen. Der Updater aktualisiert die folgenden Komponenten:

- Virendefinitionsdatei:

  Die Virendefinitionsdatei enthält die Erkennungsmuster der Schadprogramme, die Ihr Avira Produkt bei der Suche nach Viren und Malware sowie bei der Reparatur von betroffenen Objekten verwendet.

- Suchengine:

  Die Suchengine enthält die Methoden, mit denen Ihr Avira Produkt nach Viren und Malware sucht.

- Programmdateien (Produktupdate):

  Updatepakete für Produktupdates stellen weitere Funktionen für die einzelnen Programmkomponenten zur Verfügung.

Bei der Ausführung eines Updates werden die Virendefinitionsdatei, die Suchengine und die Programmdateien auf Aktualität geprüft und bei Bedarf aktualisiert. Nach einem Produktupdate kann ein Neustart Ihres Computersystems erforderlich sein. Erfolgt nur ein Update der Virendefinitionsdatei und der Suchengine, muss der Rechner nicht neu gestartet werden.

Sollte ein Neustart nach einem Produktupdate erforderlich sein, können Sie selber entscheiden, ob Sie mit der Aktualisierung fortfahren wollen oder ob Sie später wieder daran erinnert werden wollen. Wenn Sie beschließen, mit dem Update fortzufahren, werden Sie trotzdem entscheiden können, wann der Neustart stattfinden soll.

Wenn Sie zu einem späteren Zeitpunkt das Produktupdate durchführen möchten, werden trotzdem die Virendefinitionsdatei und die Suchengine aktualisiert, aber nicht die Programmdateien.

Hinweis
Das Produktupdate wird nicht abgeschlossen sein, bis ein Neustart stattgefunden hat.

Hinweis
Aus Sicherheitsgründen prüft der Updater, ob die Windows hosts-Datei Ihres Computers dahingehend geändert wurde, ob die Update-URL beispielsweise durch Malware manipuliert wurde und den Updater auf unerwünschte



Download-Seiten umleitet. Wurde die Windows hosts-Datei manipuliert, so ist dies in der Updater Reportdatei ersichtlich.

Ein Update wird in folgendem Intervall automatisch ausgeführt: 2 Stunden.

Im Control Center unter **Planer** können Sie weitere Update-Aufträge einrichten, die in den angegebenen Intervallen vom Updater ausgeführt werden. Sie haben auch die Möglichkeit, ein Update manuell zu starten:

- Im Control Center: Im Menü **Update** und in der Rubrik **Status**
- Über das Kontextmenü des Tray Icons

Sie beziehen Updates aus dem Internet über einen Webserver des Herstellers. Standardmäßig wird die existierende Netzwerkverbindung als Verbindung zu den Avira Downloadservern genutzt. Sie können diese Standardeinstellung unter Konfiguration > Update anpassen.



7. FireWall

Avira Internet Security ermöglicht Ihnen den ein- und ausgehenden Datenverkehr nach Ihren Computereinstellungen zu überwachen und zu regeln:

- Avira FireWall

Bei Betriebssystemen bis Windows 7 ist die Avira FireWall in Ihrer Avira Internet Security enthalten.

8. Backup

Sie haben verschiedene Möglichkeiten ein Backup Ihrer Daten zu erstellen:

Backup über das Backup-Tool

Mit Hilfe des Backup-Tools können Sie Backup-Profile wählen oder erstellen und ein Backup für ein ausgewähltes Profil manuell starten .

Backup über einen Backup-Auftrag im Planer

Der Planer bietet die Möglichkeit, zeitlich gesteuerte oder Ereignis gesteuerte Backup-Aufträge zu erstellen. Die Backup-Aufträge werden vom Planer automatisch ausgeführt. Dieses Verfahren eignet sich, wenn Sie regelmäßig bestimmte Daten sichern möchten .

9. Problembehebung, Tipps

In diesem Kapitel finden Sie wichtige Hinweise zur Behebung von Problemen und weitere Tipps zum Umgang mit Ihrem Avira Produkt.

- siehe Kapitel Hilfe im Problemfall
- siehe Kapitel Tastaturbefehle
- siehe Kapitel Windows Sicherheitscenter (für Windows XP) oder Windows Wartungscenter (ab Windows 7)

9.1 Hilfe im Problemfall

Hier finden Sie Informationen zu Ursachen und Lösungen möglicher Probleme.

- Die Fehlermeldung *Die Lizenzdatei lässt sich nicht öffnen* erscheint.
- Die Fehlermeldung *Der Verbindungsaufbau schlug fehl beim Downloaden der Datei ...* erscheint beim Versuch, ein Update zu starten.
- Viren und Malware können nicht verschoben oder gelöscht werden.
- Das Tray Icon zeigt einen deaktivierten Zustand an.
- Der Rechner wird extrem langsam, wenn ich eine Datensicherung durchführe.
- Meine Firewall meldet den Avira Echtzeit-Scanner und Avira Email-Schutz, sobald diese aktiv sind
- Avira Email-Schutz funktioniert nicht.
- Es ist keine Netzwerkverbindung in virtuellen Maschinen verfügbar, wenn Avira FireWall auf dem Host-Betriebssystem installiert ist und das Sicherheitsniveau der Avira FireWall auf *Mittel* bzw. *Hoch* eingestellt wurde.
- Virtual Private Network (VPN) Verbindung wird blockiert, wenn das Sicherheitsniveau der Avira FireWall auf *Mittel* bzw. *Hoch* eingestellt ist.
- Eine Email, die über eine TLS-Verbindung versendet wurde, wurde vom Email-Schutz blockiert.
- Webchat funktioniert nicht: Chat-Nachrichten werden nicht angezeigt.

Die Fehlermeldung *Die Lizenzdatei lässt sich nicht öffnen* erscheint.

Ursache: Die Datei ist verschlüsselt.

- Zur Aktivierung der Lizenz müssen Sie die Datei nicht öffnen, sondern im Programmverzeichnis speichern.



Die Fehlermeldung *Der Verbindungsaufbau schlug fehl beim Downloaden der Datei ...* erscheint beim Versuch, ein Update zu starten.

Ursache: Ihre Internetverbindung ist inaktiv. Deshalb kann keine Verbindung zum Webserver im Internet erstellt werden.

- Testen Sie, ob andere Internetdienste wie WWW oder Email funktionieren. Wenn nicht, stellen Sie die Internetverbindung wieder her.

Ursache: Der Proxyserver ist nicht erreichbar.

- Prüfen Sie, ob sich das Login für den Proxyserver geändert hat und passen Sie gegebenenfalls Ihre Konfiguration an.

Ursache: Die Datei *update.exe* ist bei Ihrer Firewall nicht vollständig freigegeben.

- Stellen Sie sicher, dass die Datei *update.exe* bei Ihrer Firewall vollständig freigegeben ist.

Ansonsten:

- Prüfen Sie in der Konfiguration unter PC Sicherheit > Update.

Viren und Malware können nicht verschoben oder gelöscht werden.

Ursache: Die Datei wurde von Windows geladen und befindet sich in einem aktiven Zustand.

- Aktualisieren Sie Ihr Avira Produkt.
- Wenn Sie das Betriebssystem Windows XP verwenden, deaktivieren Sie die Systemwiederherstellung.
- Starten Sie den Computer im abgesicherten Modus.
- Öffnen Sie die Konfiguration Ihres Avira Produkts.
- Wählen Sie **System-Scanner > Suche**, aktivieren Sie im Feld *Dateien* die Option **Alle Dateien** und bestätigen Sie das Fenster mit **OK**.
- Starten Sie einen Suchlauf über alle lokalen Laufwerke.
- Starten Sie den Computer im normalen Modus.
- Führen Sie einen Suchlauf im normalen Modus durch.
- Falls keine weiteren Viren und Malware gefunden werden, aktivieren Sie die Systemwiederherstellung, falls diese vorhanden ist und genutzt werden soll.

Das Tray Icon zeigt einen deaktivierten Zustand an.

Ursache: Der Avira Echtzeit-Scanner ist deaktiviert.

- Klicken Sie im Control Center auf den Punkt **Status** und aktivieren Sie im Bereich *PC Sicherheit* den **Echtzeit-Scanner**.

- ODER-

- Klicken Sie mit der rechten Maustaste auf das Tray Icon. Das Kontextmenü öffnet sich. Klicken Sie auf **Echtzeit-Scanner aktivieren**.

Ursache: Der Avira Echtzeit-Scanner wird von einer Firewall blockiert.

- Definieren Sie in der Konfiguration Ihrer Firewall eine generelle Freigabe für den Avira Echtzeit-Scanner. Der Avira Echtzeit-Scanner arbeitet ausschließlich mit der Adresse 127.0.0.1 (localhost). Es wird keine Verbindung ins Internet aufgebaut. Gleiches gilt für den Avira Email-Schutz.

Ansonsten:

- Überprüfen Sie die Startart des Avira Echtzeit-Scanner Dienstes. Aktivieren Sie ggf. den Dienst: Wählen Sie in der Startleiste **Start > Einstellungen >Systemsteuerung**. Starten Sie das Konfigurationsfenster **Dienste** per Doppelklick (unter Windows XP finden Sie das Dienste-Applet im Unterordner *Verwaltung*). Suchen Sie nach dem Eintrag *Avira Echtzeit-Scanner*. Als Startart muss `Automatisch` eingetragen sein und als Status `Gestartet`. Starten Sie den Dienst ggf. manuell durch Anwählen der entsprechenden Zeile und der Schaltfläche **Starten**. Tritt eine Fehlermeldung auf, überprüfen Sie bitte die Ereignisanzeige.

Der Rechner wird extrem langsam, wenn ich eine Datensicherung durchführe.

Ursache: Der Avira Echtzeit-Scanner durchsucht während des Backup-Prozesses alle Dateien, mit denen die Datensicherung arbeitet.

- Wählen Sie in der Konfiguration **Echtzeit-Scanner > Suche > Ausnahmen** und tragen Sie den Prozessnamen der Backup-Software ein.

Meine Firewall meldet den Avira Echtzeit Scanner und Avira Email-Schutz, sobald diese aktiv sind.

Ursache: Die Kommunikation des Avira Echtzeit-Scanners und Avira Email-Schutzes erfolgt über das Internetprotokoll TCP/IP. Eine Firewall überwacht alle Verbindungen über dieses Protokoll.

- Definieren Sie eine generelle Freigabe für den Avira Echtzeit-Scanner und Avira Email-Schutz. Der Avira Echtzeit-Scanner arbeitet ausschließlich mit der Adresse 127.0.0.1 (localhost). Es wird keine Verbindung ins Internet aufgebaut. Gleiches gilt für den Avira Email-Schutz.

Avira Email-Schutz funktioniert nicht.

✓ Bitte prüfen Sie die Funktionsfähigkeit des Avira Email-Schutzes anhand der folgenden Checklisten, falls in Zusammenhang mit Avira Email-Schutz Probleme auftreten.

Checkliste

✓ Prüfen Sie, ob Ihr Mail Client sich per Kerberos, APOP oder RPA beim Server



anmeldet. Diese Authentifizierungsmethoden werden derzeit nicht unterstützt.

- ✓ Prüfen Sie, ob sich Ihr Mail Client per SSL (auch häufig TLS - Transport Layer Security - genannt) am Server anmeldet. Avira Email-Schutz unterstützt kein SSL und beendet daher die SSL verschlüsselte Verbindungen. Falls Sie SSL verschlüsselte Verbindungen ohne Schutz des Avira Email-Schutzes verwenden möchten, müssen Sie für die Verbindung einen anderen Port nutzen als die vom Email-Schutz überwachten Ports. Die vom Email-Schutz überwachten Ports können in der Konfiguration unter **Email-Schutz > Suche** konfiguriert werden.
- ✓ Ist der Avira Email-Schutz Dienst (Service) aktiv? Aktivieren Sie ggf. den Dienst: Wählen Sie in der Startleiste **Start > Einstellungen > Systemsteuerung**. Starten Sie das Konfigurationsfenster **Dienste** per Doppelklick (unter Windows XP finden Sie das Dienste-Applet im Unterordner *Verwaltung*). Suchen Sie nach dem Eintrag *Avira Email-Schutz*. Als Startart muss `Automatisch` eingetragen sein und als Status `Gestartet`. Starten Sie den Dienst ggf. manuell durch Anwählen der entsprechenden Zeile und der Schaltfläche **Starten**. Tritt eine Fehlermeldung auf, überprüfen Sie bitte die *Ereignisanzeige*. Ist dies nicht von Erfolg gekrönt, sollten Sie ggf. das Avira Produkt über **Start > Einstellungen > Systemsteuerung > Software** komplett deinstallieren, den Rechner neu starten und Ihr Avira Produkt anschließend neu installieren.

Allgemeines

- Über SSL (Secure Sockets Layer) verschlüsselte POP3 Verbindungen (auch häufig als TLS (Transport Layer Security) bezeichnet) können derzeit nicht geschützt werden und werden ignoriert.
- Authentifizierung zum Mail Server wird derzeit nur über Passworte unterstützt. "Kerberos" und "RPA" werden derzeit nicht unterstützt.
- Ihr Avira Produkt prüft Emails beim Versenden nicht auf Viren und unerwünschte Programme.

> **Hinweis**
> Wir empfehlen Ihnen, regelmäßig Microsoft Updates durchzuführen, um eventuelle Sicherheitslücken zu schließen.

Es ist keine Netzwerkverbindung in virtuellen Maschinen verfügbar, wenn Avira FireWall auf dem Host-Betriebssystem installiert ist und das Sicherheitsniveau der Avira FireWall auf *Mittel* bzw. *Hoch* eingestellt wurde.

Wenn die Avira FireWall auf einem Computer installiert ist, auf dem zusätzlich eine virtuelle Maschine (beispielsweise VMWare, Virtual PC, u.a.) betrieben wird, blockiert diese alle Netzwerkverbindungen der virtuellen Maschine, wenn das Sicherheitsniveau der Avira FireWall auf *Mittel* bzw. *Hoch* eingestellt wurde. Beim Sicherheitsniveau *Niedrig* werden die Netzverbindungen von der FireWall zugelassen.

Ursache: Die virtuelle Maschine emuliert per Software eine Netzwerkkarte. Durch diese Emulation werden die Datenpakete des Gastsystems in spezielle (sog. UDP) Pakete



gekapselt und über das externe Gateway zurück zum Host-System geroutet. In der Avira FireWall werden ab dem Sicherheitsniveau *Mittel* diese von außen kommenden Pakete blockiert.

Um dieses Verhalten zu umgehen gehen Sie wie folgt vor:

- Wählen Sie im Control Center die Rubrik *INTERNET SICHERHEIT* **> FireWall**.
- Klicken Sie auf den Link **Konfiguration**.
- Das Dialogfenster *Konfiguration* erscheint. Sie befinden Sich in der Konfigurationsrubrik *Anwendungsregeln*.
- Wählen Sie die Konfigurationsrubrik **Adapterregeln**.
- Klicken Sie auf **Hinzufügen**.
- Wählen Sie unter *Eingehende Regel* **UDP**.
- Geben Sie der Regel im Bereich *Name der Regel* einen **Namen**.
- Klicken Sie **OK**.
- Prüfen Sie, ob die Regel eine Prioritätsstufe über der Regel **Alle IP-Pakete zurückweisen** liegt.

> **Warnung**
> Diese Regel birgt potentielle Gefahren in sich, da sie grundsätzlich UDP-Pakete erlaubt! Wechseln Sie nach dem Betrieb Ihrer virtuellen Maschine wieder in Ihr vorheriges Sicherheitsniveau.

Virtual Private Network (VPN) Verbindung wird blockiert, wenn das Sicherheitsniveau der Avira FireWall auf *Mittel* bzw. *Hoch* eingestellt ist.

Ursache: Standardmäßig werden alle Pakete, die den voreingestellten Regeln nicht entsprechen, nicht zugelassen. Die durch die VPN-Software versendeten Pakete werden durch diese Regeln gefiltert, da sie aufgrund Ihres Typs (sog. GRE-Pakete) in keine der anderen Kategorien fallen.

- Fügen Sie bei den **Adapterregeln** der Avira FireWall-Konfiguration die Regel **VPN-Verbindungen erlauben** hinzu, um alle VPN bezogenen Pakete zuzulassen.

Eine Email, die über eine TLS-Verbindung versendet wurde, wurde vom Email-Schutz blockiert.

Ursache: Transport Layer Security (TLS: Verschlüsselungsprotokoll für Datenübertragungen im Internet) wird derzeit nicht vom Email-Schutz unterstützt. Sie haben folgende Möglichkeiten die Email zu senden:

- Nutzen Sie einen anderen Port als den von SMTP genutzten Port 25. Sie umgehen damit die Überwachung durch den Email-Schutz.



- Verzichten Sie auf die TLS verschlüsselte Verbindung und deaktivieren Sie die TLS-Unterstützung in Ihrem Email-Client.
- Deaktivieren Sie (vorübergehend) die Überwachung der ausgehenden Emails durch den Email-Schutz in der Konfiguration unter **Email-Schutz > Suche**.

Webchat funktioniert nicht: Chat-Nachrichten werden nicht angezeigt.

Dieses Phänomen kann bei Chats auftreten, die auf dem HTTP-Protokoll mit 'transfer-encoding: chunked' basieren.

Ursache: Der Browser-Schutz prüft gesendete Daten zunächst vollständig auf Viren und unerwünschte Programme, bevor die Daten im Webbrowser geladen werden. Bei einem Datentransfer mit 'transfer-encoding: chunked' kann der Browser-Schutz die Nachrichtenlänge bzw. die Datenmenge nicht ermitteln.

- Geben Sie in der Konfiguration die URL des Webchats als Ausnahme an (siehe Konfiguration: Browser-Schutz > Suche > Ausnahmen).

9.2 Tastaturbefehle

Tastaturbefehle - auch Shortcuts genannt - bieten eine schnelle Möglichkeit durch das Programm zu navigieren, einzelne Module aufzurufen und Aktionen zu starten.

Im Folgenden erhalten Sie eine Übersicht über die verfügbaren Tastaturbefehle. Nähere Hinweise zur Funktionalität und Verfügbarkeit finden Sie im entsprechenden Kapitel der Hilfe.

9.2.1 In Dialogfeldern

Tastaturbefehl	Beschreibung
Strg + Tab **Strg + Bild runter**	Navigation im Control Center Zur nächsten Rubrik wechseln.
Strg + Umsch + Tab **Strg + Bild runter**	Navigation im Control Center Zur vorherigen Rubrik wechseln.

←↑→↓	Navigation in den Konfigurationsrubriken Setzen Sie zunächst den Fokus mit der Maus auf eine Konfigurationsrubrik. Zwischen den Optionen in einem markierten Drop-Down-Listenfeld oder zwischen mehreren Optionen in einer Optionsgruppe wechseln.
Tab	Zur nächsten Option oder Optionsgruppe wechseln.
Umsch + Tab	Zur vorherigen Option oder Optionsgruppe wechseln.
Leertaste	Aktivieren bzw. Deaktivieren eines Kontrollkästchens, wenn die aktive Option ein Kontrollkästchen ist.
Alt + unterstrichener Buchstabe	Option wählen bzw. Befehl ausführen.
Alt + ↓ **F4**	Ausgewähltes Drop-Down-Listenfeld öffnen.
Esc	Ausgewähltes Drop-Down-Listenfeld schließen. Befehl abbrechen und Dialogfeld schließen.
Eingabetaste	Befehl für die aktive Option oder Schaltfläche ausführen.

9.2.2 In der Hilfe

Tastaturbefehl	Beschreibung
Alt + Leertaste	Systemmenü anzeigen.
Alt + Tab	Umschalten zwischen der Hilfe und anderen geöffneten Fenstern.

Alt + F4	Hilfe schließen.
Umschalt + F10	Kontextmenüs der Hilfe anzeigen.
Strg + Tab	Zur nächsten Rubrik im Navigationsfenster wechseln.
Strg + Umsch + Tab	Zur vorherigen Rubrik im Navigationsfenster wechseln.
Bild hoch	Zum Thema wechseln, das oberhalb des aktuellen Themas im Inhaltsverzeichnis, im Index oder in der Liste der Suchergebnisse angezeigt wird.
Bild runter	Zum Thema wechseln, das unterhalb des aktuellen Themas im Inhaltsverzeichnis, im Index oder in der Liste der Suchergebnisse angezeigt wird.
Bild hoch **Bild runter**	Durch ein Thema blättern.

9.2.3 Im Control Center

Allgemein

Tastaturbefehl	Beschreibung
F1	Hilfe anzeigen
Alt + F4	Control Center schließen
F5	Ansicht aktualisieren
F8	Konfiguration öffnen
F9	Update starten

Rubrik **System-Scanner**

Tastaturbefehl	Beschreibung
F2	Ausgewähltes Profil umbenennen
F3	Suchlauf mit dem ausgewählten Profil starten
F4	Desktopverknüpfung für das ausgewählte Profil erstellen
Einf	Neues Profil erstellen
Entf	Ausgewähltes Profil löschen

Rubrik **FireWall**

Tastaturbefehl	Beschreibung
Enter	Eigenschaften

Rubrik **Quarantäne**

Tastaturbefehl	Beschreibung
F2	Objekt erneut prüfen
F3	Objekt wiederherstellen
F4	Objekt senden
F6	Objekt wiederherstellen nach...
Enter	Eigenschaften
Einf	Datei hinzufügen
Entf	Objekt löschen

Rubrik **Planer**



Tastaturbefehl	Beschreibung
F2	Auftrag ändern
Enter	Eigenschaften
Einf	Neuen Auftrag einfügen
Entf	Auftrag löschen

Rubrik **Berichte**

Tastaturbefehl	Beschreibung
F3	Reportdatei anzeigen
F4	Reportdatei drucken
Enter	Bericht anzeigen
Entf	Bericht(e) löschen

Rubrik **Ereignisse**

Tastaturbefehl	Beschreibung
F3	Ereignis(se) exportieren
Enter	Ereignis anzeigen
Entf	Ereignis(se) löschen

9.3 Windows Sicherheitscenter

- Windows XP Service Pack 2 -



9.3.1 Allgemeines

Das Windows Sicherheitscenter überprüft den Status eines Computers im Hinblick auf wichtige Sicherheitsaspekte.

Wenn bei einem dieser wichtigen Punkte ein Problem festgestellt wird (z.B. ein veraltetes Antivirenprogramm), sendet das Sicherheitscenter eine Warnung und stellt Empfehlungen bereit, wie Sie den Computer besser schützen können.

9.3.2 Das Windows Sicherheitscenter und Ihr Avira Produkt

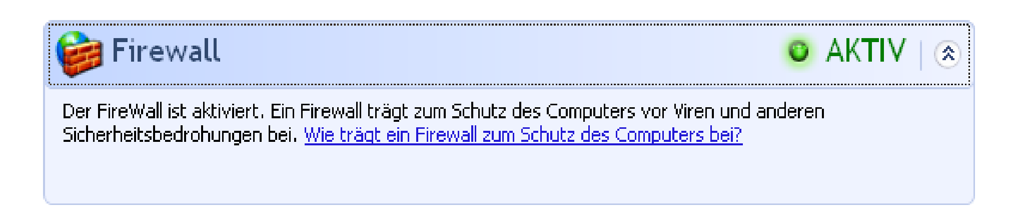
Firewall

Es ist möglich, dass Sie vom Sicherheitscenter die folgende firewallbezogene Information erhalten:

- Firewall AKTIV / Firewall ein
- Firewall INAKTIV / Firewall aus

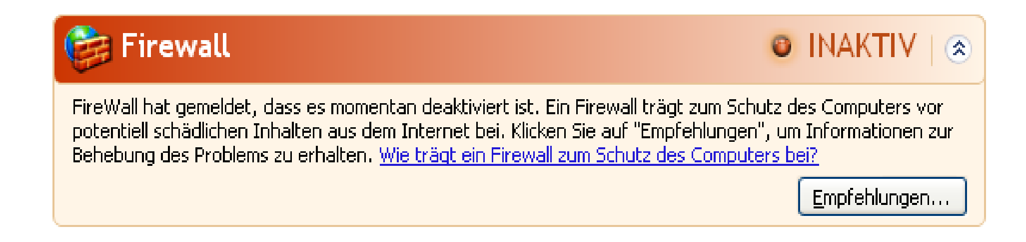
Firewall AKTIV / Firewall ein

Nach der Installation Ihres Avira Produkts und dem Abschalten der Windows-Firewall erhalten Sie die folgende Meldung:



Firewall INAKTIV / Firewall aus

Sie erhalten die folgende Meldung, sobald Sie die Avira FireWall deaktivieren:



Hinweis
Sie können die Avira FireWall über **Status** im **Control Center** aktivieren bzw. deaktivieren.



Warnung
Wenn Sie die Avira FireWall deaktivieren, ist Ihr Computer nicht länger vor dem unautorisierten Zugriff über das Netzwerk oder das Internet geschützt.

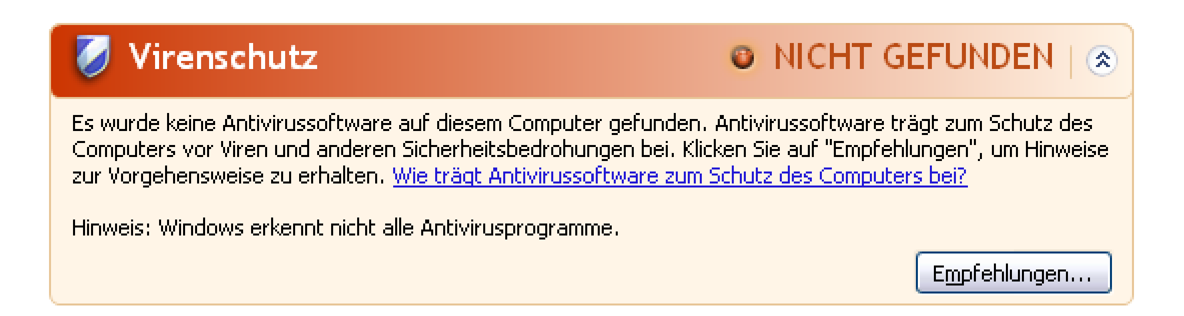
Virenschutzsoftware / Schutz vor schädlicher Software

Folgende Hinweise können Sie in Bezug auf Ihren Virenschutz vom Windows Sicherheitscenter erhalten.

- Virenschutz NICHT GEFUNDEN
- Virenschutz NICHT AKTUELL
- Virenschutz AKTIV
- Virenschutz INAKTIV
- Virenschutz NICHT ÜBERWACHT

Virenschutz NICHT GEFUNDEN

Dieser Hinweis des Windows Sicherheitscenters erscheint, wenn das Windows Sicherheitscenter keine Antivirensoftware auf Ihrem Computer gefunden hat.

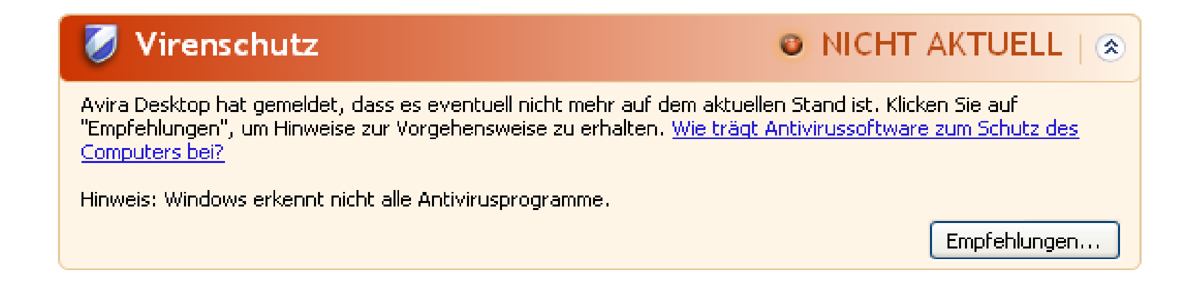


Hinweis
Installieren Sie Ihr Avira Produkt auf Ihrem Computer, um diesen vor Viren und sonstigen unerwünschten Programmen zu schützen!

Virenschutz NICHT AKTUELL

Haben Sie Windows XP Service Pack 2 bereits installiert und installieren danach Ihr Avira Produkt oder aber installieren Sie Windows XP Service Pack 2 auf ein System, auf dem Ihr Avira Produkt bereits installiert war erhalten Sie folgende Meldung:

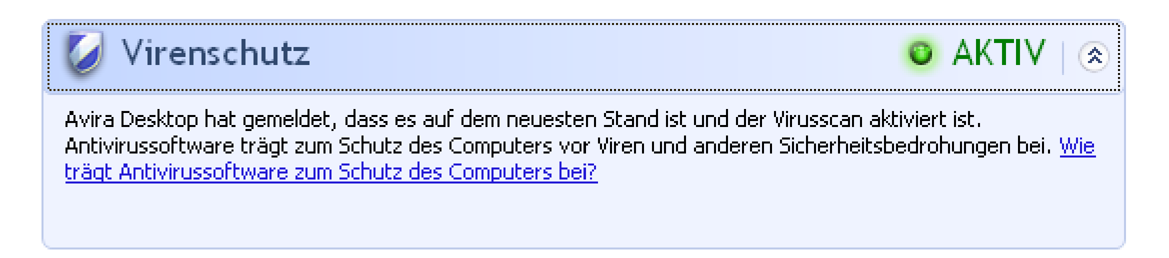




Hinweis
Damit das Windows Sicherheitscenter Ihr Avira Produkt als aktuell erkennt, ist nach der Installation zwingend ein Update erforderlich. Sie aktualisieren Ihr System, indem Sie ein Update durchführen.

Virenschutz AKTIV

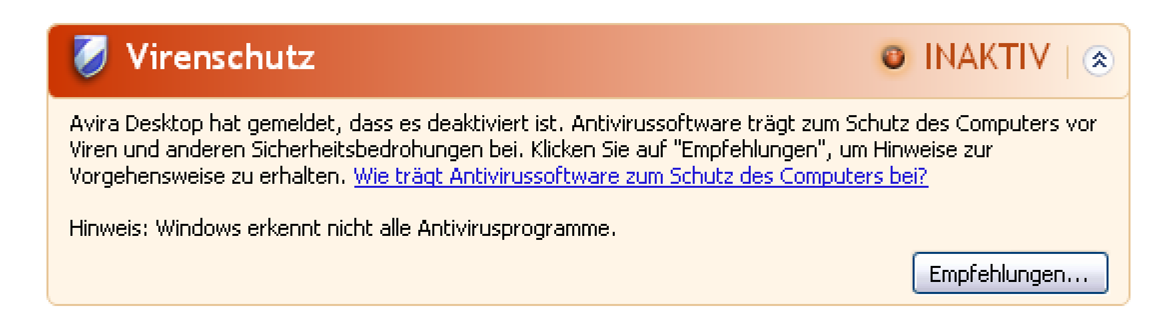
Nach der Installation Ihres Avira Produkts und einem im Anschluss daran durchgeführten Update erhalten Sie folgenden Hinweis:



Ihr Avira Produkt ist nun auf aktuellem Stand und der Avira Echtzeit-Scanner ist aktiv.

Virenschutz INAKTIV

Nachfolgenden Hinweis erhalten Sie, wenn Sie den Avira Echtzeit-Scanner deaktivieren oder aber den Echtzeit-Scanner Dienst stoppen.

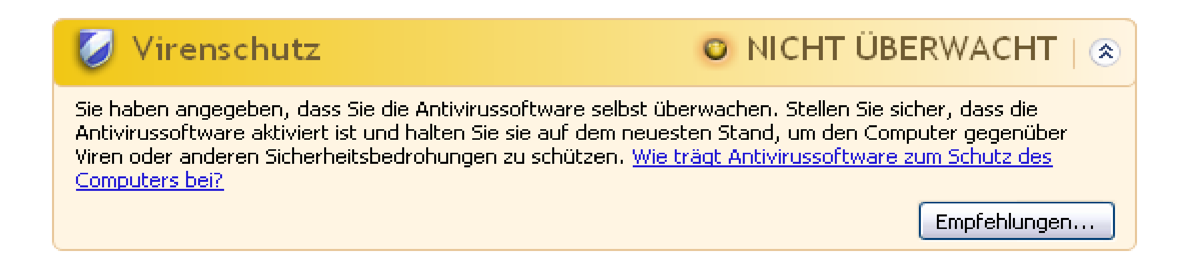


Hinweis
Den Avira Echtzeit-Scanner können Sie unter der Rubrik **Status** des **Control Centers** aktivieren bzw. deaktivieren. Sie erkennen zudem, dass der Avira

Echtzeit-Scanner aktiviert ist, wenn der rote Regenschirm in Ihrer Taskleiste geöffnet ist.

Virenschutz NICHT ÜBERWACHT

Erhalten Sie folgenden Hinweis vom Windows Sicherheitscenter, dann haben Sie sich dafür entschieden, dass Sie Ihre Antivirensoftware selbst überwachen.



Hinweis
Das Windows Sicherheitscenter wird von Ihrem Avira Produkt unterstützt. Sie können diese Option jederzeit über die Schaltfläche **Empfehlungen...** aktivieren.

Hinweis
Auch wenn Sie Windows XP Service Pack 2 installiert haben benötigen Sie weiterhin eine Virenschutzlösung. Obwohl Windows Ihre Antivirensoftware überwacht, enthält es selbst keinerlei Antivirus-Funktionen. Sie wären also ohne eine zusätzliche Virenschutzlösung nicht vor Viren und sonstiger Malware geschützt!

9.4 Windows Wartungscenter

- Windows 7 und Windows 8 -

9.4.1 Allgemeines

Hinweis:
Das **Windows Sicherheitscenter** wurde ab Windows 7 in **Windows Wartungscenter** umbenannt. Unter diesem Programmabschnitt finden Sie jetzt den Status aller Ihrer Sicherheits-Optionen.

Das Windows Wartungscenter überprüft den Status eines Computers im Hinblick auf wichtige Sicherheitsaspekte. Sie können direkt auf das Wartungscenter zugreifen, indem



Sie auf die kleine Flagge in Ihrer Taskleiste klicken oder unter **Systemsteuerung > Wartungscenter**.

Wenn bei einem dieser wichtigen Punkte ein Problem festgestellt wird (z.B. ein veraltetes Antivirenprogramm), sendet das Wartungscenter eine Warnung und stellt Empfehlungen bereit, wie Sie den Computer besser schützen können. Das bedeutet, wenn alles richtig funktioniert, werden Sie keine Meldung vom Wartungscenter erhalten. Trotzdem ist es möglich, den Sicherheitsstatus des Computers im **Wartungscenter** unter der Rubrik **Sicherheit** zu beobachten.
Es wird Ihnen auch die Möglichkeit gegeben, die Programme, die Sie installiert haben, zu verwalten und auszuwählen (z.B. *Antispywareprogramme auf dem Computer anzeigen*).

Sie können die Warnmeldungen unter **Wartungscenter > Einstellungen ändern** (z.B. *Meldungen zum Schutz vor Spyware und ähnlicher Malware deaktivieren*) ausschalten.

9.4.2 Das Windows Wartungscenter und Ihr Avira Produkt

Netzwerkfirewall

Es ist möglich, dass Sie vom Wartungscenter die folgende firewallbezogene Information erhalten:

- Avira FireWall hat gemeldet, dass es eingeschaltet ist
- Sowohl Windows-Firewall als auch Avira FireWall haben gemeldet, dass sie ausgeschaltet sind
- Die Windows-Firewall ist deaktiviert oder nicht richtig eingerichtet

Avira FireWall hat gemeldet, dass es eingeschaltet ist

Nach der Installation Ihres Avira Produkts und dem Abschalten der Windows-Firewall erhalten Sie die folgende Meldung unter **Wartungscenter > Sicherheit > Netzwerkfirewall**: *Avira FireWall hat gemeldet, dass es eingeschaltet ist*. Das bedeutet, dass Avira FireWall Ihre gewählte Firewall-Lösung ist (beachten Sie bitte den Unterschied zwischen Firewall (Windows Produkt) und FireWall (Aviras Produkt)).

> **Warnung**
> Mit **Windows-Firewall** ist **nicht** Ihre **Avira FireWall** gemeint. Deshalb sollten Sie sich keine Sorgen machen, falls Sie folgende Meldungen bekommen: *Firewalleinstellungen aktualisieren* oder ***Die zum Schutz des Computers empfohlenen Einstellungen werden nicht von der Windows-Firewall verwendet.*** **Ihr Avira Produkt funktioniert problemlos und Ihr Computer ist sicher**. Windows informiert Sie einfach nur darüber, dass seine eigenen Programme ausgeschaltet sind.



Firewalleinstellungen aktualisieren

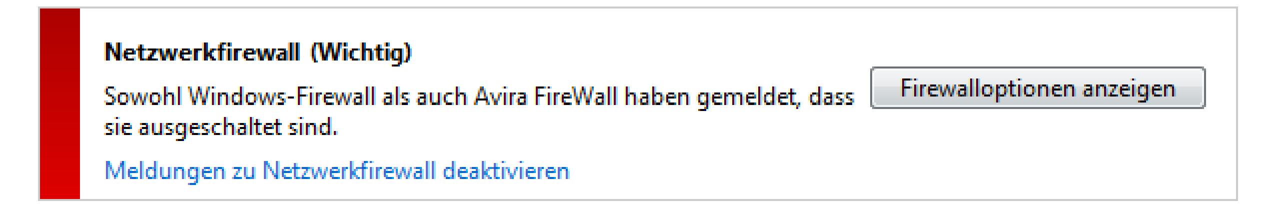
Die zum Schutz des Computers empfohlenen Einstellungen werden nicht von der Windows-Firewall verwendet.

Empfohlene Einstellungen

Was sind die empfohlenen Einstellungen?

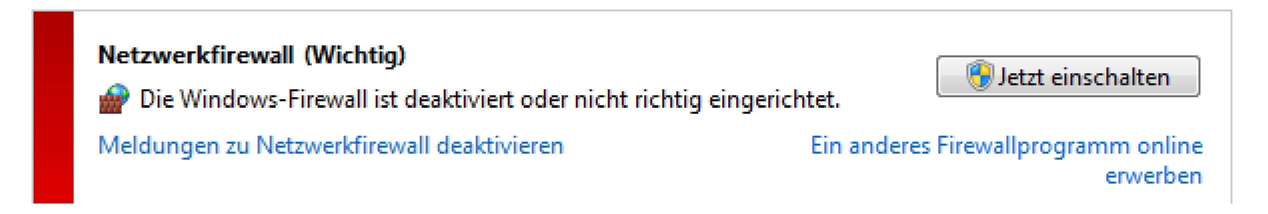
Sowohl Windows-Firewall als auch Avira FireWall haben gemeldet, dass sie ausgeschaltet sind

Sie erhalten die folgende Meldung, sobald Sie die Avira FireWall deaktivieren:



Warnung
Wenn Sie die **Avira FireWall** deaktivieren, ist Ihr Computer nicht länger vor dem unautorisierten Zugriff über das Netzwerk oder das Internet geschützt.

Die Windows-Firewall ist deaktiviert oder nicht richtig eingerichtet



Das bedeutet, dass weder die **Windows-Firewall** noch die **Avira FireWall** aktiviert sind.

- **Unter Windows 7**

  Die Avira FireWall ist deaktiviert oder nicht richtig eingerichtet. Avira FireWall sollte durch das Wartungscenter automatisch erkannt werden. Bitte führen Sie einen Neustart durch. Sollte das Problem weiterhin bestehen, installieren Sie das Avira Produkt erneut.

Virenschutz

Folgende Hinweise können Sie in Bezug auf Ihren Virenschutz vom Windows Wartungscenter erhalten:

- Avira Desktop hat gemeldet, dass es auf dem neuesten Stand ist und die Virenerkennung eingeschaltet ist



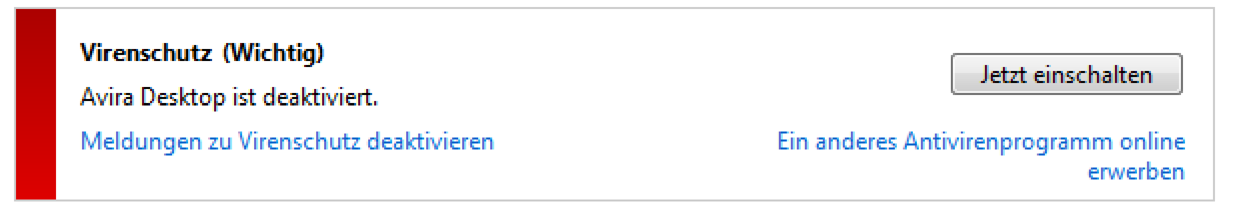
- Avira Desktop ist deaktiviert
- Avira Desktop ist nicht mehr aktuell
- Es wurde keine Antivirensoftware auf dem Computer gefunden
- Ihr PC ist nicht mehr durch Avira Desktop geschützt

Avira Desktop hat gemeldet, dass es auf dem neuesten Stand ist und die Virenerkennung eingeschaltet ist

Nach der Installation Ihres Avira Produkts und einem im Anschluss daran durchgeführten Update werden Sie zunächst keine Meldungen vom Windows Wartungscenter erhalten. Sie können jedoch unter **Wartungscenter > Sicherheit** folgenden Hinweis finden: *"Avira Desktop" hat gemeldet, dass es auf dem neuesten Stand ist und die Virenerkennung eingeschaltet ist*. Das heißt, dass Ihr Avira Produkt nun auf aktuellem Stand ist und der Avira Echtzeit-Scanner aktiv ist.

Avira Desktop ist deaktiviert

Nachfolgenden Hinweis erhalten Sie, wenn Sie den Avira Echtzeit-Scanner deaktivieren oder aber den Echtzeit-Scanner Dienst stoppen.



> **Hinweis**
> Den **Avira Echtzeit-Scanner** können Sie unter der Rubrik **Status** des **Avira Control Centers** aktivieren bzw. deaktivieren. Sie können zudem erkennen, ob der **Avira Echtzeit-Scanner** aktiviert ist, wenn der rote Regenschirm in Ihrer Taskleiste geöffnet ist. Es ist auch möglich, die einzelnen Avira Komponenten durch das Anklicken der *Jetzt einschalten*-Taste des Wartungscenters zu aktivieren. Wenn Sie eine Meldung erhalten sollten, bei der Sie Ihre Zustimmung geben müssen, das Avira Programm laufen zu lassen, klicken Sie auf *Zulassen* und der Echtzeit-Scanner wird aktiviert.

Avira Desktop ist nicht mehr aktuell

Wenn Sie gerade Avira installiert haben, oder wenn aus irgendeinen Grund die Virendefinitionsdatei, die Suchengine oder die Programmdateien Ihres Avira Produkts nicht automatisch aktualisiert wurden (z.B. wenn Sie von einer älteren Version eines Windows Betriebssystems, auf dem Ihr Avira Produkt bereits installiert ist, auf eine neuere Version upgraden), erhalten Sie folgende Meldung:

Virenschutz (Wichtig)
"Avira Desktop" ist nicht mehr aktuell.
Meldungen zu Virenschutz deaktivieren
Jetzt aktualisieren
Ein anderes Antivirenprogramm online erwerben

Hinweis
Damit das Windows Wartungscenter Ihr Avira Produkt als aktuell erkennt, ist nach der Installation zwingend ein Update erforderlich. Sie aktualisieren Ihr System, indem Sie ein Update durchführen.

Es wurde keine Antivirensoftware auf dem Computer gefunden

Dieser Hinweis des Windows Wartungscenters erscheint, wenn das Windows Wartungscenter keine Antivirensoftware auf Ihrem Computer gefunden hat.

Virenschutz (Wichtig)
Es wurde keine Antivirensoftware auf dem Computer gefunden.
Meldungen zu Virenschutz deaktivieren
Programm online suchen

Hinweis
Bitte beachten Sie, dass diese Option nicht in Windows 8 verfügbar ist. Windows Defender ist ab diesem Betriebssystem die von Microsoft voreingestellte Virenschutzfunktion.

Hinweis
Installieren Sie Ihr Avira Produkt auf Ihrem Computer, um diesen vor Viren und sonstigen unerwünschten Programmen zu schützen!

Ihr PC ist nicht mehr durch Avira Desktop geschützt

Dieser Hinweis des Windows Wartungscenters erscheint, wenn die Lizenz Ihres Avira Produkts abgelaufen ist.
Wenn Sie auf die Schaltfläche **Aktion ausführen** klicken, werden Sie auf die Avira Webseite weitergeleitet, wo Sie eine neue Lizenz erwerben können.

Virenschutz (Wichtig)
Ihr PC ist nicht mehr durch Avira Desktop geschützt.
Meldungen zu Virenschutz deaktivieren
Aktion ausführen
Installierte Antiviren-Apps anzeigen



Hinweis
Bitte beachten Sie, dass diese Option nur für Windows 8 verfügbar ist.

Schutz vor Spyware und unerwünschter Software

Folgende Hinweise können Sie in Bezug auf Ihren Schutz vor Spyware und unerwünschter Software vom Windows Wartungscenter erhalten:

- Avira Desktop hat gemeldet, dass es eingeschaltet ist
- Sowohl Windows Defender als auch Avira Desktop haben gemeldet, dass sie ausgeschaltet sind
- Avira Desktop ist nicht mehr aktuell
- Windows Defender ist nicht mehr aktuell
- Windows Defender ist ausgeschaltet

Avira Desktop hat gemeldet, dass es eingeschaltet ist

Nach der Installation Ihres Avira Produkts und einem im Anschluss daran durchgeführten Update werden Sie zunächst keine Meldungen vom Windows Wartungscenter erhalten. Sie können jedoch unter **Wartungscenter > Sicherheit** folgenden Hinweis finden: *"Avira Desktop" hat gemeldet, dass es eingeschaltet ist*. Das heißt, dass Ihr Avira Produkt auf aktuellem Stand ist und der Avira Echtzeit-Scanner aktiv ist.

Sowohl Windows Defender als auch Avira Desktop haben gemeldet, dass sie ausgeschaltet sind

Nachfolgenden Hinweis erhalten Sie, wenn Sie den Avira Echtzeit-Scanner deaktivieren oder aber den Dienst des Avira Echtzeit-Scanners stoppen.

Schutz vor Spyware und unerwünschter Software (Wichtig)
Sowohl Windows Defender als auch Avira Desktop haben gemeldet, dass sie ausgeschaltet sind.
Meldungen zu Schutz vor Spyware und ähnlicher Malware deaktivieren
Antispywareprogramme anzeigen

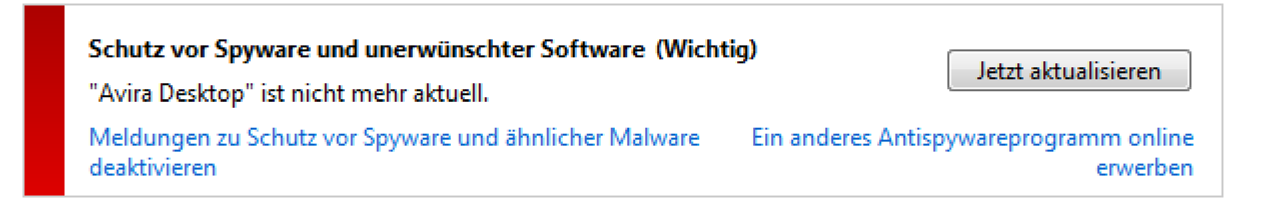
Hinweis
Den **Avira Echtzeit-Scanner** können Sie unter der Rubrik **Status** des **Avira Control Centers** aktivieren bzw. deaktivieren. Sie können zudem erkennen, ob der **Avira Echtzeit-Scanner** aktiviert ist, wenn der rote Regenschirm in Ihrer Taskleiste geöffnet ist. Es ist auch möglich, die einzelnen Avira Komponenten durch das Anklicken der *Jetzt einschalten*-Taste des Wartungscenters zu aktivieren. Wenn Sie eine Meldung erhalten sollten, bei der Sie Ihre



Zustimmung geben müssen, das Avira Programm laufen zu lassen, klicken Sie auf *Zulassen* und der Echtzeit-Scanner wird aktiviert.

Avira Desktop ist nicht mehr aktuell

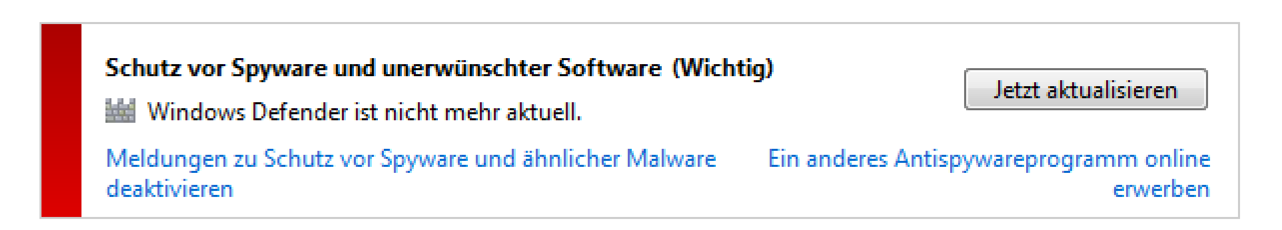
Wenn Sie gerade Avira installiert haben, oder wenn aus irgendeinem Grund die Virendefinitionsdatei, die Suchengine oder die Programmdateien Ihres Avira Produkts nicht automatisch aktualisiert wurden (z.B. wenn Sie von einer älteren Version eines Windows Betriebssystems, auf dem Ihr Avira Produkt bereits installiert ist, auf eine neuere Version upgraden), erhalten Sie folgende Meldung:



Hinweis
Damit das Windows Wartungscenter Ihr Avira Produkt als aktuell erkennt, ist nach der Installation zwingend ein Update erforderlich. Sie aktualisieren Ihr System, indem Sie ein Update durchführen.

Windows Defender ist nicht mehr aktuell

Die folgende Meldung kann angezeigt werden, wenn Windows Defender aktiviert ist. Das könnte bedeuten, dass Ihr Avira Produkt nicht richtig installiert wurde. Bitte überprüfen Sie dies.



Hinweis
Windows Defender ist die vordefinierte Spyware- und Virenschutz-Lösung von Windows.

Windows Defender ist ausgeschaltet

Sie erhalten die Meldung des Windows Wartungscenters *Windows Defender ist ausgeschaltet*, wenn keine andere Antispyware-Software auf Ihrem Computer gefunden wurde. Windows Defender ist eine von Microsoft im Betriebssystem standardmäßig integrierte Software zur Erkennung von Spyware. Wenn Sie schon eine andere

Antivirensoftware auf Ihrem Computer installiert hatten, wurde diese Anwendung deaktiviert.
Ist das Avira Produkt richtig installiert, sollten Sie diese Meldung nicht erhalten, denn das Wartungscenter erkennt Avira automatisch. Bitte überprüfen Sie, ob Avira richtig funktioniert.

Schutz vor Spyware und unerwünschter Software (Wichtig)
Windows Defender ist ausgeschaltet.
Jetzt einschalten
Meldungen zu Schutz vor Spyware und ähnlicher Malware deaktivieren
Ein anderes Antispywareprogramm online erwerben

10. Viren und mehr

Avira Internet Security erkennt nicht nur Viren und Malware, das Produkt kann Sie auch vor weiteren Gefahren schützen. In diesem Kapitel finden Sie einen Überblick über die verschiedenen Arten von Malware sowie über andere Gefahren. Dieser beschreibt sowohl woher sie kommen und ihr Verhalten als auch die unliebsamen Überraschungen, die damit auf Sie zukommen.

Verwandte Themen:

- Gefahrenkategorien
- Viren sowie sonstige Malware

10.1 Gefahrenkategorien

Adware

Als Adware wird Software bezeichnet, die dem Benutzer zusätzlich zur eigentlichen Funktionalität Werbe-Banner oder Werbe-Popups zeigt. Diese Werbeeinblendungen lassen sich in der Regel nicht abschalten und sind meist immer sichtbar. Hier erlauben die Verbindungsdaten bereits vielfältige Rückschlüsse auf das Nutzungsverhalten und sind aus Datenschutzgründen problematisch.

Ihr Avira Produkt erkennt Adware. Ist in der Konfiguration unter Gefahrenkategorien die Option **Adware** aktiviert, erhalten Sie eine entsprechende Warnmeldung, wenn Ihr Avira Produkt solche Software entdeckt.

Adware/Spyware

Software, die Werbung einblendet oder Software, die persönliche Daten des Anwenders häufig ohne dessen Wissen oder Zustimmung an Dritte versendet und daher möglicherweise unerwünscht ist.

Ihr Avira Produkt erkennt "Adware/Spyware". Ist in der Konfiguration unter Gefahrenkategorien die Option **Adware/Spyware** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt fündig geworden ist.

Anwendung

Bei der Bezeichnung Anwendung handelt es sich um eine Applikation, deren Nutzung mit einem Risiko verbunden sein kann oder die von fragwürdiger Herkunft ist.
Ihr Avira Produkt erkennt "Anwendung" (APPL). Ist in der Konfiguration unter Gefahrenkategorien die Option **Anwendung** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt ein solches Verhalten bemerkt.

Backdoor-Steuersoftware

Um Daten zu stehlen oder Rechner zu manipulieren, wird "durch die Hintertür" ein Backdoor-Server-Programm eingeschleust, ohne dass der Anwender es merkt. Über Internet oder Netzwerk kann dieses Programm über eine Backdoor-Steuersoftware (Client) von Dritten gesteuert werden.
Ihr Avira Produkt erkennt "Backdoor-Steuersoftware". Ist in der Konfiguration unter Gefahrenkategorien die Option **Backdoor-Steuersoftware** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt fündig geworden ist.

Dateien mit verschleierten Dateiendungen

Ausführbare Dateien, die ihre wahre Dateiendung in verdächtiger Weise verschleiern. Diese Methode der Verschleierung wird häufig von Malware benutzt.
Ihr Avira Produkt erkennt "Dateien mit verschleierten Dateiendungen". Ist in der Konfiguration unter Gefahrenkategorien die Option **Dateien mit verschleierten Dateiendungen** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt fündig geworden ist.

Kostenverursachendes Einwahlprogramm

Bestimmte im Internet angebotene Dienstleistungen sind kostenpflichtig. Die Abrechnung erfolgt in Deutschland über Einwahlprogramme mit 0190/0900-Nummern (in Österreich und der Schweiz über 09x0-Nummern; in Deutschland wird mittelfristig auf 09x0 umgestellt). Auf dem Rechner installiert, gewährleisten diese Programme - kurz Dialer genannt - den Verbindungsaufbau über eine entsprechende Premium-Rate-Nummer, deren Tarifgestaltung ein breites Spektrum umfassen kann.

Die Vermarktung von Online-Inhalten über den Weg der Telefonrechnung ist legal und kann für den Nutzer vorteilhaft sein. Seriöse Dialer lassen deshalb keinen Zweifel daran aufkommen, dass sie vom Kunden bewusst und mit Bedacht eingesetzt werden. Sie installieren sich nur dann auf dem Anwender-Rechner, wenn der Nutzer dazu seine Zustimmung abgibt, wobei diese Zustimmung aufgrund einer völlig eindeutigen und klar erkennbaren Etikettierung bzw. Aufforderung erfolgt sein muss. Der Verbindungsaufbau seriöser Dialer-Programme wird unmissverständlich angezeigt. Außerdem informieren seriöse Dialer exakt und augenfällig über die Höhe der dabei entstehenden Kosten.

Leider jedoch gibt es Dialer, die sich unauffällig, auf fragwürdige Weise oder gar in betrügerischer Absicht auf Rechnern installieren. Sie ersetzen z.B. die Standard-DFÜ-Verbindung des Internet-Nutzers zum ISP (Internet-Service-Provider) und rufen bei jeder Verbindung eine kostenverursachende, oft horrend überteuerte 0190/0900-Nummer an. Der betroffene Anwender merkt mitunter erst mit der nächsten Telefonrechnung, dass ein unerwünschtes 0190/0900-Dialer-Programm auf seinem Rechner bei jedem Verbindungsaufbau zum Internet eine Premium-Rate-Nummer gewählt hat - mit der Folge drastisch hoher Gebühren.

Um sich generell vor unerwünschten kostenverursachenden Einwahlprogrammen (0190/0900-Dialern) zu schützen, empfehlen wir Ihnen, sich direkt bei Ihrem Telefon-Anbieter für diesen Nummernkreis sperren zu lassen.

Standardmäßig erkennt Ihr Avira Produkt die ihm bekannten kostenverursachende Einwahlprogramme.

Ist in der Konfiguration unter Gefahrenkategorien die Option **Kostenverursachendes Einwahlprogramm** mit einem Häkchen aktiviert, erhalten Sie bei Auffinden eines kostenverursachenden Einwahlprogramms einen entsprechenden Warnhinweis. Sie haben nun die Möglichkeit, den eventuell unerwünschten 0190/0900-Dialer einfach zu löschen. Ist dies allerdings ein erwünschtes Einwahlprogramm, können Sie es als Ausnahmedatei deklarieren und diese Datei wird dann zukünftig nicht mehr untersucht.

Phishing

Phishing, auch bekannt als "brand spoofing" ist eine raffinierte Form des Datendiebstahls, der auf Kunden bzw. potienzielle Kunden von Internet Service Providern, Banken, Online-Banking Diensten, Registrierungsbehörden abzielt.
Durch eine Weitergabe der eigenen Email-Adresse im Internet, das Ausfüllen von Online-Formularen, dem Beitritt von Newsgroups oder Webseiten ist es möglich, dass Ihre Daten von sog. "Internet crawling spiders" gestohlen und ohne Ihre Erlaubnis dazu verwendet werden einen Betrug oder andere Verbrechen zu begehen.

Ihr Avira Produkt erkennt "Phishing". Ist in der Konfiguration unter Gefahrenkategorien die Option **Phishing** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt ein solches Verhalten bemerkt.

Programme, die die Privatsphäre verletzen

Software, die die Sicherheit Ihres Systems beeinträchtigen, nicht gewünschte Programmaktivitäten auslösen, Ihre Privatsphäre verletzen oder Ihr Benutzerverhalten ausspähen kann und daher möglicherweise unerwünscht ist.

Ihr Avira Produkt erkennt "Security Privacy Risk" Software. Ist in der Konfiguration unter Gefahrenkategorien die Option **Programme, die die Privatsphäre verletzen** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt fündig geworden ist.

Scherzprogramme

Die Scherzprogramme sollen lediglich jemanden erschrecken oder zur allgemeinen Belustigung dienen, ohne schädlich zu sein oder sich selbst zu vermehren. Meist fängt der Computer nach dem Aufruf eines Witzprogramms irgendwann an, eine Melodie zu spielen oder etwas Ungewohntes auf dem Bildschirm zu zeigen. Beispiele für Witzprogramme sind die Waschmaschine im Diskettenlaufwerk (DRAIN.COM) und der Bildschirmfresser (BUGSRES.COM).

Aber Vorsicht! Alle Symptome von Scherzprogrammen könnten auch von einem Virus oder einem Trojaner stammen. Zumindest bekommt man aber einen gehörigen Schreck oder richtet in Panik hinterher sogar selbst tatsächlichen Schaden an.

Ihr Avira Produkt ist in der Lage, durch die Erweiterung seiner Such- und Identifikationsroutinen Witzprogramme zu erkennen und sie als unerwünschtes Programm ggf. zu eliminieren. Ist in der Konfiguration unter Gefahrenkategorien die Option **Scherzprogramme** mit einem Häkchen aktiviert, wird über entsprechende Funde informiert.

Spiele

Computerspiele müssen sein - aber sie gehören nicht unbedingt an den Arbeitsplatz (die Mittagspause vielleicht einmal ausgenommen). Dennoch wird von Mitarbeitern in Unternehmen und Behörden so manches Moorhuhn erlegt und so mancher Karobube doppelgeklickt. Über das Internet kann eine Fülle von Spielen heruntergeladen werden. Auch Email-Games erfreuen sich wachsender Verbreitung: Vom simplen Schach bis zum "Flottenmanöver" (inklusive Torpedogefecht) sind zahlreiche Varianten in Umlauf: Die jeweiligen Spielzüge werden über Mailprogramme an Partner gesendet und von diesen beantwortet.

Untersuchungen haben ergeben, dass die zum Computerspielen verwendete Arbeitszeit längst wirtschaftlich relevante Größenordnungen erreicht hat. Umso verständlicher ist, dass immer mehr Unternehmen Möglichkeiten in Betracht ziehen, Computerspiele von Arbeitsplatzrechnern fern zu halten.

Ihr Avira Produkt erkennt Computerspiele. Ist in der Konfiguration unter Gefahrenkategorien die Option **Spiele** mit einem Häkchen aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt fündig geworden ist. Das Spiel ist nun im wahrsten Sinne des Wortes aus, denn Sie haben die Möglichkeit, es einfach zu löschen.

Trügerische Software

Auch als "Scareware" (Schreckprogramme) oder "Rogueware" (Schurkenprogramme) bekannt, bezeichnet betrügerische Software, die Vireninfektionen und Gefahren vorgaukelt und dabei professioneller Antivirensoftware täuschend ähnlich sieht. Scareware ist darauf ausgelegt, den Benutzer zu verunsichern oder zu verängstigen. Fällt das Opfer auf den Trick herein und glaubt sich bedroht, wird ihm häufig gegen Bezahlung eine Beseitigung der nicht vorhandenen Gefahr angeboten. In anderen Fällen soll das Opfer durch den Glauben an einen erfolgreichen Angriff zu Handlungen verleitet werden, welche einen tatsächlichen Angriff erst ermöglichen.

Ist in der Konfiguration unter Gefahrenkategorien die Option **Trügerische Software** mit einem Häkchen aktiviert, erhalten Sie bei Auffinden von Scareware einen entsprechenden Warnhinweis.

Ungewöhnliche Laufzeitpacker

Dateien, die mit einem ungewöhnlichen Laufzeitpacker komprimiert wurden und daher als möglicherweise verdächtig eingestuft werden können.

Ihr Avira Produkt erkennt "Ungewöhnliche Laufzeitpacker". Ist in der Konfiguration unter Gefahrenkategorien die Option **Ungewöhnliche Laufzeitpacker (PCK)** aktiviert, erhalten Sie eine entsprechende Warnung, wenn Ihr Avira Produkt fündig geworden ist.

10.2 Viren sowie sonstige Malware

Adware

Als Adware wird Software bezeichnet, die dem Benutzer zusätzlich zur eigentlichen Funktionalität Werbe-Banner oder Werbe-Popups zeigt. Diese Werbeeinblendungen lassen sich in der Regel nicht abschalten und sind meist immer sichtbar. Hier erlauben die Verbindungsdaten bereits vielfältige Rückschlüsse auf das Nutzungsverhalten und sind aus Datenschutzgründen problematisch.

Backdoors

Einem Backdoor (deutsch: Hintertür) ist es möglich, unter Umgehung der Zugriffssicherung, Zugriff auf einen Computer zu erlangen.

Ein versteckt laufendes Programm ermöglicht einem Angreifer meist fast uneingeschränkte Rechte. Mit Hilfe des Backdoors können persönliche Daten des Anwenders ausspioniert werden. Aber Sie werden meist dazu benutzt, weitere Computerviren oder Würmer auf dem betroffenen System zu installieren.

Bootviren

Der Boot- bzw. Masterbootsektor von Festplatten wird mit Vorliebe von Bootsektorviren infiziert. Sie überschreiben wichtige Informationen zum Systemstart. Eine der unangenehmen Folgen: das Betriebssystem kann nicht mehr geladen werden...

Bot-Net

Unter einem Bot-Net versteht man ein fernsteuerbares Netzwerk (im Internet) von PCs, welches aus untereinander kommunizierenden Bots besteht. Diese Kontrolle wird durch Viren bzw. Trojaner erreicht, die den Computer infizieren und dann auf Anweisungen warten, ohne auf dem infizierten Rechner Schaden anzurichten. Diese Netzwerke können für Spam-Verbreitung, DDoS Attacken, usw. verwendet werden, z.T. ohne dass die betroffenen PC-Nutzer etwas merken. Das Hauptpotenzial von Bot-Nets besteht darin, dass die Netzwerke Größen von tausenden Rechnern erreichen können, deren Bandbreitensumme die der meisten herkömmlichen Internetzugänge sprengt.

Exploit

Ein Exploit (Sicherheitslücke) ist ein Computerprogramm oder Script, welches spezifische Schwächen oder Fehlfunktionen eines Betriebssystems oder Programms ausnutzt. Eine Form des Exploits sind Angriffe aus dem Internet mit Hilfe von manipulierten Datenpaketen, die Schwachstellen in der Netzwerksoftware ausnutzen. Hier können Programme eingeschleust werden, mit denen ein größerer Zugriff erlangt werden kann.

Hoaxes (engl.: hoax - Scherz, Schabernack, Ulk)

Seit ein paar Jahren erhalten die User im Internet und in anderen Netzen Warnungen vor Viren, die sich angeblich per Email verbreiten sollen. Diese Warnungen werden über Email mit der Aufforderung verbreitet, sie an möglichst viele Kollegen und andere Benutzer weiter zu senden, um alle vor der "Gefahr" zu warnen.

Honeypot

Ein Honeypot (Honigtopf) ist ein in einem Netzwerk installierter Dienst (Programm oder Server). Dieser hat die Aufgabe, ein Netzwerk zu überwachen und Angriffe zu protokollieren. Dieser Dienst ist dem legitimen Nutzer unbekannt und wird daher niemals angesprochen. Wenn nun ein Angreifer ein Netzwerk auf Schwachstellen untersucht und dabei die von einem Honeypot angebotenen Dienste in Anspruch nimmt, wird er protokolliert und ein Alarm ausgelöst.

Makroviren

Makroviren sind kleine Programme, die in der Makrosprache einer Anwendung (z.B. WordBasic unter WinWord 6.0) geschrieben sind und sich normalerweise auch nur innerhalb von Dokumenten dieser Anwendung verbreiten können. Sie werden deshalb auch Dokumentviren genannt. Damit sie aktiv werden, sind sie immer darauf angewiesen, dass die entsprechende Applikation gestartet und eines der infizierten Makros ausgeführt wird. Im Unterschied zu "normalen" Viren befallen Makroviren also keine ausführbaren Dateien sondern die Dokumente der jeweiligen Wirts-Applikation.

Pharming

Pharming ist eine Manipulation der Hostdatei von Webbrowsern, um Anfragen auf gefälschte Webseiten umzuleiten. Es handelt sich um eine Weiterentwicklung des klassischen Phishings. Pharming-Betrüger unterhalten eigene große Server-Farmen, auf denen gefälschte Webseiten abgelegt sind. Pharming hat sich auch als Oberbegriff für verschiedene Arten von DNS-Angriffen etabliert. Bei einer Manipulation der Host-Datei wird unter Zuhilfenahme eines Trojaners oder eines Virus eine gezielte Manipulation des Systems vorgenommen. Die Folge davon ist, dass von diesem System nur noch gefälschte Websites abrufbar sind, selbst wenn die Web-Adresse korrekt eingegeben wurde.

Phishing

Phishing bedeutet ins Deutsche übersetzt das Fischen nach persönlichen Daten des Internetnutzers. Der Phisher schickt seinem Opfer in der Regel offiziell wirkende Schreiben, wie beispielsweise Emails, die es verleiten sollen, vertrauliche Informationen, vor allem Benutzernamen und Passwörter oder PIN und TAN von Online-Banking-Zugängen, im guten Glauben dem Täter preiszugeben. Mit den gestohlenen Zugangsdaten kann der Phisher die Identität seines Opfers übernehmen und in dessen Namen Handlungen ausführen. Klar ist: Banken und Versicherungen bitten niemals um die Zusendung von Kreditkartennummern, PIN, TAN oder anderen Zugangsdaten per Email, per SMS oder telefonisch.

Polymorphe Viren

Wahre Meister der Tarnung und Verkleidung sind polymorphe Viren. Sie verändern ihre eigenen Programmiercodes - und sind deshalb besonders schwer zu erkennen.

Programmviren

Ein Computervirus ist ein Programm, welches die Fähigkeit besitzt, sich nach seinem Aufruf selbsttätig an andere Programme auf irgendeine Weise anzuhängen und dadurch zu infizieren. Viren vervielfältigen sich also im Gegensatz zu logischen Bomben und Trojanern selber. Im Gegensatz zu einem Wurm benötigt der Virus immer ein fremdes Programm als Wirt, in dem er seinen virulenten Code ablegt. Im Normalfall wird aber der eigentliche Programmablauf des Wirtes selber nicht geändert.

Rootkits

Unter Rootkits versteht man eine Sammlung von Softwarewerkzeugen, die nach dem Einbruch in ein Computersystem installiert werden, um Logins des Eindringlings zu verbergen, Prozesse zu verstecken und Daten mitzuschneiden - generell gesagt: sich unsichtbar zu machen. Sie versuchen bereits installierte Spionageprogramme zu aktualisieren und gelöschte Spyware erneut zu installieren.

Skriptviren und Würmer

Diese Viren sind extrem einfach zu programmieren und verbreiten sich - entsprechende Techniken vorausgesetzt - innerhalb weniger Stunden per Email um den ganzen Erdball.

Skriptviren und -würmer benutzen eine der Script-Sprachen, wie beispielsweise Javascript, VBScript etc., um sich selbst in andere, neue Skripte einzufügen oder sich selber durch den Aufruf von Betriebssystemfunktionen zu verbreiten. Häufig geschieht dies per Email oder durch den Austausch von Dateien (Dokumenten).

Als Wurm wird ein Programm bezeichnet, das sich selber vervielfältigt jedoch keinen Wirt infiziert. Würmer können also nicht Bestandteil anderer Programmabläufe werden.

Würmer sind auf Systemen mit restriktiveren Sicherheitsvorkehrungen oft die einzige Möglichkeit irgendwelche Schadensprogramme einzuschleusen.

Spyware

Spyware sind sogenannte Spionageprogramme, die persönliche Daten des Benutzers ohne dessen Wissen oder gar Zustimmung an den Hersteller der Software oder an Dritte sendet. Meist dienen Spyware-Programme dazu, das Surf-Verhalten im Internet zu analysieren und gezielte Werbe-Banner oder Werbe-Popups einzublenden.

Trojanische Pferde (kurz Trojaner)

Trojaner sind in letzter Zeit recht häufig anzutreffen. So bezeichnet man Programme, die vorgeben, eine bestimmte Funktion zu haben, nach ihrem Start aber ihr wahres Gesicht zeigen und irgendeine andere Funktion ausführen, die zumeist zerstörerisch ist. Trojanische Pferde können sich nicht selber vermehren, was sie von Viren und Würmern unterscheidet. Die meisten haben einen interessanten Namen (SEX.EXE oder STARTME.EXE), der den Anwender zur Ausführung des Trojaners verleiten soll. Unmittelbar nach der Ausführung werden diese dann aktiv und formatieren z.B. die Festplatte. Eine spezielle Art eines Trojaners ist ein Dropper, der Viren 'droppt', d.h. in das Computersystem einpflanzt.

Trügerische Software

Auch als "Scareware" (Schreckprogramme) oder "Rogueware" (Schurkenprogramme) bekannt, bezeichnet betrügerische Software, die Vireninfektionen und Gefahren vorgaukelt und dabei professioneller Antivirensoftware täuschend ähnlich sieht. Scareware ist darauf ausgelegt, den Benutzer zu verunsichern oder zu verängstigen. Fällt das Opfer auf den Trick herein und glaubt sich bedroht, wird ihm häufig gegen Bezahlung eine Beseitigung der nicht vorhandenen Gefahr angeboten. In anderen Fällen soll das Opfer durch den Glauben an einen erfolgreichen Angriff zu Handlungen verleitet werden, welche einen tatsächlichen Angriff erst ermöglichen.

Zombie

Ein Zombie-PC ist ein Rechner, welcher mit Malwareprogrammen infiziert ist und es den Hackern erlaubt, Rechner per Fernsteuerung für ihre kriminellen Zwecke zu missbrauchen. Der betroffene PC startet auf Befehl beispielsweise Denial-of-Service-(DoS) Attacken oder versendet Spam und Phishing Emails.

11. Info und Service

In diesem Kapitel erhalten Sie Informationen, auf welchen Wegen Sie mit uns in Kontakt treten können.

- siehe Kapitel Kontaktadresse
- siehe Kapitel Technischer Support
- siehe Kapitel Verdächtige Datei
- siehe Kapitel Fehlalarm melden
- siehe Kapitel Ihr Feedback für mehr Sicherheit

11.1 Kontaktadresse

Gerne helfen wir Ihnen weiter, wenn Sie Fragen und Anregungen zur Avira Produktwelt haben. Unsere Kontaktadressen finden Sie im Control Center unter **Hilfe > Über Avira Internet Security**.

11.2 Technischer Support

Der Avira Support steht Ihnen zuverlässig zur Seite, wenn es gilt, Ihre Fragen zu beantworten oder ein technisches Problem zu lösen.

Auf unserer Webseite erhalten Sie alle nötigen Informationen zu unserem umfangreichen Support-Service:
http://www.avira.de/premium-suite-support

Damit wir Ihnen schnell und zuverlässig helfen können, sollten Sie die folgenden Informationen bereithalten:

- **Lizenzdaten**. Diese finden Sie auf der Programmoberfläche unter dem Menüpunkt **Hilfe > Über Avira Internet Security > Lizenzinformationen**. Siehe Lizenzinformationen.
- **Versionsinformationen**. Diese finden Sie auf der Programmoberfläche unter dem Menüpunkt **Hilfe > Über Avira Internet Security > Versionsinformationen**. Siehe Versionsinformationen.
- **Betriebssystemversion** und eventuell installierte Service-Packs.
- **Installierte Software-Pakete**, z.B. Antivirensoftware anderer Hersteller.
- **Genaue Meldungen** des Programms oder der Reportdatei.

11.3 Verdächtige Datei

Sie können verdächtige Dateien oder Viren, die gegebenenfalls von unseren Produkten noch nicht erkannt bzw. entfernt werden können, an uns senden. Dafür stellen wir Ihnen mehrere Wege zur Verfügung.

- Wählen Sie die Datei im Quarantänemanager des Control Centers aus und wählen Sie über das Kontextmenü oder die entsprechende Schaltfläche den Punkt **Datei senden**.
- Senden Sie die gewünschte Datei gepackt (WinZIP, PKZip, Arj, etc.) im Anhang einer Email an folgende Adresse:
  virus-premium-suite@avira.de
  Da einige Email-Gateways mit Antivirensoftware arbeiten, sollten Sie die Datei(en) zusätzlich mit einem Kennwort versehen (bitte nicht vergessen, uns das Kennwort mitzuteilen).
- Alternativ haben Sie die Möglichkeit, die verdächtige Datei über unsere Webseite an uns zu senden: http://www.avira.de/sample-upload

11.4 Fehlalarm melden

Sind Sie der Meinung, dass Ihr Avira Produkt einen Fund in einer Datei meldet, die jedoch mit hoher Wahrscheinlichkeit "sauber" ist, so senden Sie diese Datei, gepackt (WinZIP, PKZIP, Arj, etc.) im Anhang einer Email, an folgende Adresse:
virus-premium-suite@avira.de

Da einige Email-Gateways mit Antivirensoftware arbeiten, sollten Sie die Datei(en) zusätzlich mit einem Kennwort versehen (bitte nicht vergessen, uns das Kennwort mitzuteilen).

11.5 Ihr Feedback für mehr Sicherheit

Bei Avira steht die Sicherheit unserer Kunden an erster Stelle. Aus diesem Grund beschäftigen wir nicht nur ein eigenes Expertenteam, welches jede einzelne Avira Lösung und jedes einzelne Update vor der Veröffentlichung aufwendigen Qualitäts- und Sicherheitstests unterzieht. Für uns gehört auch dazu, Hinweise auf eventuell auftretende, sicherheitsrelevante Schwachstellen ernst zu nehmen und mit diesen offen umzugehen.

Wenn Sie glauben, eine sicherheitsrelevante Schwachstelle in einem unserer Produkte gefunden zu haben, senden Sie bitte eine Email an folgende Adresse:

vulnerabilities-premium-suite@avira.de



12. Referenz: Konfigurationsoptionen

Die Referenz der Konfiguration dokumentiert alle verfügbaren Konfigurationsoptionen.

12.1 System-Scanner

Die Rubrik **System-Scanner** der Konfiguration ist für die Konfiguration der Direktsuche, d.h. für die Suche auf Verlangen, zuständig.

12.1.1 Suche

Sie können hier das grundlegende Verhalten der Suchroutine bei einer Direktsuche festlegen. Wenn Sie bei der Direktsuche bestimmte Verzeichnisse für die Prüfung wählen, prüft der System-Scanner je nach Konfiguration:

- mit einer bestimmten Suchleistung (Priorität),
- zusätzlich Bootsektoren und Hauptspeicher,
- alle oder ausgewählte Dateien im Verzeichnis.

Dateien

Der System-Scanner kann einen Filter verwenden, um nur Dateien mit einer bestimmten Endung (Typ) zu prüfen.

Alle Dateien

Bei aktivierter Option werden alle Dateien, unabhängig von ihrem Inhalt und ihrer Dateierweiterung, nach Viren bzw. unerwünschten Programmen durchsucht. Der Filter wird nicht verwendet.

> **Hinweis**
> Ist **Alle Dateien** aktiv, lässt sich die Schaltfläche **Dateierweiterungen** nicht anwählen.

Intelligente Dateiauswahl

Bei aktivierter Option wird die Auswahl der zu prüfenden Dateien vollautomatisch vom Programm übernommen. D.h. Ihr Avira Produkt entscheidet anhand des Inhalts einer Datei, ob diese auf Viren und unerwünschte Programme geprüft werden soll oder nicht. Dieses Verfahren ist etwas langsamer als **Dateierweiterungsliste verwenden**, aber wesentlich sicherer, da nicht nur anhand der Dateierweiterung geprüft wird. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

> **Hinweis**
> Ist **Intelligente Dateiauswahl** aktiv, lässt sich die Schaltfläche **Dateierweiterungen** nicht anwählen.

Dateierweiterungsliste verwenden

Bei aktivierter Option werden nur Dateien mit einer vorgegebenen Endung durchsucht. Voreingestellt sind alle Dateitypen, die Viren und unerwünschte Programme enthalten können. Die Liste lässt sich über die Schaltfläche "**Dateierweiterungen"** manuell editieren.

> **Hinweis**
> Ist diese Option aktiv und Sie haben alle Einträge aus der Liste mit Dateiendungen gelöscht, wird dies durch den Text "*Keine Dateierweiterungen*" unterhalb der Schaltfläche **Dateierweiterungen** angezeigt.

Dateierweiterungen

Mit Hilfe dieser Schaltfläche wird ein Dialogfenster aufgerufen, in dem alle Dateiendungen angezeigt werden, die bei einem Suchlauf im Modus "**Dateierweiterungsliste verwenden"** untersucht werden. Bei den Endungen sind Standardeinträge vorgegeben, es lassen sich aber auch Einträge hinzufügen oder entfernen.

> **Hinweis**
> Beachten Sie bitte, dass sich die Standardliste von Version zu Version ändern kann.

Weitere Einstellungen

Bootsektor Suchlaufwerke

Bei aktivierter Option prüft der System-Scanner die Bootsektoren der bei der Direktsuche gewählten Laufwerke. Diese Einstellung ist standardmäßig aktiviert.

Masterbootsektoren durchsuchen

Bei aktivierter Option prüft der System-Scanner die Masterbootsektoren der im System verwendeten Festplatte(n).

Offline Dateien ignorieren

Bei aktivierter Option ignoriert die Direktsuche sog. Offline Dateien bei einem Suchlauf komplett. D.h., diese Dateien werden nicht auf Viren und unerwünschte Programme geprüft. Offline Dateien sind Dateien, die durch ein sog. Hierarchisches Speicher-Management-System (HSMS) physikalisch von der Festplatte auf z.B. ein Band ausgelagert wurden. Diese Einstellung ist standardmäßig aktiviert.



Integritätsprüfung von Systemdateien

Bei aktivierter Option werden bei jeder Direktsuche die wichtigsten Windows Systemdateien einer besonders sicheren Prüfung auf Veränderungen durch Malware unterzogen. Wird eine veränderte Datei gefunden, wird diese als verdächtiger Fund gemeldet. Die Funktion nimmt viel Rechnerleistung in Anspruch. Daher ist die Option standardmäßig deaktiviert.

> **Hinweis**
> Die Option ist nur ab Windows Vista verfügbar.

> **Hinweis**
> Falls Sie Drittanbieter Tools einsetzen, die Systemdateien verändern und den Boot- oder Startbildschirm auf eigene Bedürfnisse anpassen, sollten Sie diese Option nicht verwenden. Beispiele für diese Tools sind sogenannte Skinpacks, TuneUp Utilities oder Vista Customization.

Optimierter Suchlauf

Bei aktivierter Option wird die Prozessor-Kapazität bei einem Suchlauf des System-Scanners optimal ausgelastet. Aus Gründen der Performance erfolgt die Protokollierung beim optimierten Suchlauf höchstens auf einem Standard-Level.

> **Hinweis**
> Die Option ist nur bei Multi-Prozessor-Rechnern verfügbar.

Symbolischen Verknüpfungen folgen

Bei aktivierter Option folgt der System-Scanner bei einer Suche allen symbolischen Verknüpfungen im Suchprofil oder ausgewählten Verzeichnis, um die verknüpften Dateien nach Viren und Malware zu durchsuchen.

> **Hinweis**
> Die Option schließt keine Dateiverknüpfungen (Shortcuts) ein, sondern bezieht sich ausschließlich auf symbolische Links (erzeugt mit mklink.exe) oder Junction Points (erzeugt mit junction.exe), die transparent im Dateisystem vorliegen.

Rootkits-Suche bei Suchstart

Bei aktivierter Option prüft der System-Scanner bei einem Suchstart in einem sog. Schnellverfahren das Windows-Systemverzeichnis auf aktive Rootkits. Dieses Verfahren prüft Ihren Rechner nicht so umfassend auf aktive Rootkits wie das

Suchprofil "**Suche nach Rootkits"**, ist jedoch in der Ausführung bedeutend schneller. Diese Option ändert nur die Einstellungen der von Ihnen selbst erstellten Profile.

Hinweis
Die Rootkits-Suche ist unter Windows XP 64 Bit nicht verfügbar!

Registry durchsuchen

Bei aktivierter Option wird bei einem Suchlauf die Registry nach Verweisen auf Schadsoftware durchsucht. Diese Option ändert nur die Einstellungen der von Ihnen selbst erstellten Profile.

Dateien und Pfade auf Netzlaufwerken ignorieren

Bei aktivierter Option sind mit dem Computer verbundene Netzlaufwerke von der Direktsuche ausgenommen. Diese Option empfiehlt sich, wenn die Server oder andere Workstations selbst durch eine Antiviren-Software geschützt werden. Diese Option ist standardmäßig deaktiviert.

Suchvorgang

Stoppen zulassen

Bei aktivierter Option, lässt sich die Suche nach Viren oder unerwünschten Programmen jederzeit mit der Schaltfläche "**Stopp"** im Fenster "**Luke Filewalker**" beenden. Haben Sie diese Einstellung deaktiviert, wird die Schaltfläche **Stopp** im Fenster "**Luke Filewalker**" grau unterlegt. Das vorzeitige Beenden eines Suchlaufs ist so nicht möglich! Diese Einstellung ist standardmäßig aktiviert.

Scanner-Priorität

Der System-Scanner unterscheidet bei der Direktsuche drei Prioritätsstufen. Dies ist nur wirksam, wenn auf dem Computer mehrere Prozesse gleichzeitig ablaufen. Die Wahl wirkt sich auf die Suchgeschwindigkeit aus.

niedrig

Der System-Scanner erhält vom Betriebssystem nur dann Prozessorzeit zugewiesen, wenn kein anderer Prozess Rechenzeit benötigt, d.h. solange der System-Scanner alleine läuft, ist die Geschwindigkeit maximal. Insgesamt wird die Arbeit mit anderen Programmen dadurch sehr gut ermöglicht: Der Computer reagiert schneller, wenn andere Programme Rechenzeit benötigen, während dann der System-Scanner im Hintergrund weiterläuft.

mittel

Der System-Scanner wird mit normaler Priorität ausgeführt. Alle Prozesse erhalten vom Betriebssystem gleich viel Prozessorzeit zugewiesen. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen. Unter Umständen ist die Arbeit mit anderen Anwendungen beeinträchtigt.

hoch

Der System-Scanner erhält höchste Priorität. Ein paralleles Arbeiten mit anderen Anwendungen ist kaum mehr möglich. Jedoch erledigt der System-Scanner seinen Suchlauf maximal schnell.

Aktion bei Fund

Sie können Aktionen festlegen, die der System-Scanner ausführen soll, wenn ein Virus oder unerwünschtes Programm gefunden wurde.

Interaktiv

Bei aktivierter Option werden Funde der Suche des System-Scanners in einem Dialogfenster gemeldet. Bei der Suche des System-Scanners erhalten Sie beim Abschluss des Suchlaufs eine Warnmeldung mit einer Liste der gefundenen betroffenen Dateien. Sie haben die Möglichkeit, über das Kontextmenü eine auszuführende Aktion für die einzelnen betroffenen Dateien auszuwählen. Sie können die gewählten Aktionen für alle betroffenen Dateien ausführen oder den System-Scanner beenden.

> **Hinweis**
> Standardmäßig ist im Dialogfenster zur Virenbehandlung die Aktion **Quarantäne** vorausgewählt. Über ein Kontextmenü können Sie weitere Aktionen auswählen.

Automatisch

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms kein Dialog, in dem eine Aktion ausgewählt werden kann. Der System-Scanner reagiert nach den von Ihnen in diesem Abschnitt vorgenommenen Einstellungen.

Datei vor Aktion in Quarantäne kopieren

Bei aktivierter Option erstellt der System-Scanner eine Sicherheitskopie (Backup) vor der Durchführung der gewünschten primären bzw. sekundären Aktion. Die Sicherheitskopie wird in der Quarantäne aufbewahrt, wo die Datei wiederhergestellt werden kann, wenn sie einen informativen Wert hat. Zudem können Sie die Sicherheitskopie für weitere Untersuchungen an das Avira Malware Research Center senden.

Primäre Aktion

Primäre Aktion, ist die Aktion die ausgeführt wird, wenn der System-Scanner einen Virus bzw. ein unerwünschtes Programm findet. Ist die Option "**Reparieren"** gewählt, jedoch eine Reparatur der betroffenen Datei nicht möglich, wird die unter "**Sekundäre Aktion"** gewählte Aktion ausgeführt.

Hinweis
Die Option **Sekundäre Aktion** ist nur dann auswählbar, wenn unter **Primäre Aktion** die Einstellung **Reparieren** ausgewählt wurde.

Reparieren

Bei aktivierter Option repariert der System-Scanner betroffene Dateien automatisch. Wenn der System-Scanner eine betroffene Datei nicht reparieren kann, führt er alternativ die unter Sekundäre Aktion gewählte Option aus.

Hinweis
Eine automatische Reparatur wird empfohlen, bedeutet aber, dass der System-Scanner Dateien auf dem Computer verändert.

Umbenennen

Bei aktivierter Option benennt der System-Scanner die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurück benannt werden.

Quarantäne

Bei aktivierter Option verschiebt der System-Scanner die Datei in Quarantäne. Diese Dateien können später repariert oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Löschen

Bei aktivierter Option wird die Datei gelöscht. Dieser Vorgang ist bedeutend schneller als **Überschreiben und löschen** (siehe unten).

Ignorieren

Bei aktivierter Option wird der Zugriff auf die Datei erlaubt und die Datei belassen.

Warnung
Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Überschreiben und löschen

Bei aktivierter Option überschreibt der System-Scanner die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

Sekundäre Aktion

Die Option "**Sekundäre Aktion"** ist nur dann auswählbar, wenn unter "**Primäre Aktion"** die Einstellung **Reparieren** ausgewählt wurde. Mittels dieser Option kann nun entschieden werden, was mit der betroffenen Datei geschehen soll, wenn diese nicht reparabel ist.



Umbenennen

Bei aktivierter Option benennt der System-Scanner die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurück benannt werden.

Quarantäne

Bei aktivierter Option verschiebt der System-Scanner die Datei in Quarantäne. Diese Dateien können später repariert oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Löschen

Bei aktivierter Option wird die Datei gelöscht. Dieser Vorgang ist bedeutend schneller als "Überschreiben und löschen".

Ignorieren

Bei aktivierter Option wird der Zugriff auf die Datei erlaubt und die Datei belassen.

Warnung
Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Überschreiben und löschen

Bei aktivierter Option überschreibt der System-Scanner die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

Hinweis
Wenn Sie als primäre oder sekundäre Aktion **Löschen** oder **Überschreiben und löschen** ausgewählt haben, beachten Sie bitte folgendes: Bei heuristischen Treffern werden die betroffenen Dateien nicht gelöscht, sondern in die Quarantäne verschoben.

Archive

Bei der Suche in Archiven wendet der System-Scanner eine rekursive Suche an: Es werden auch Archive in Archiven entpackt und auf Viren und unerwünschte Programme geprüft. Die Dateien werden geprüft, dekomprimiert und noch einmal geprüft.

Archive durchsuchen

Bei aktivierter Option werden die in der Archiv-Liste markierten Archive geprüft. Diese Einstellung ist standardmäßig aktiviert.

Alle Archiv-Typen

Bei aktivierter Option werden alle Archivtypen in der Archiv-Liste markiert und geprüft.

Smart Extensions

Bei aktivierter Option erkennt der System-Scanner, ob es sich bei einer Datei um ein gepacktes Dateiformat (Archiv) handelt, auch wenn die Dateiendung von den gebräuchlichen Endungen abweicht, und prüft das Archiv. Dafür muss jedoch jede Datei geöffnet werden - was die Suchgeschwindigkeit verringert. Beispiel: Wenn ein *.zip-Archiv mit der Dateiendung *.xyz versehen ist, entpackt der System-Scanner auch dieses Archiv und prüft es. Diese Einstellung ist standardmäßig aktiviert.

> **Hinweis**
> Es werden nur diejenigen Archivtypen geprüft, die in der Archiv-Liste markiert sind.

Rekursionstiefe einschränken

Das Entpacken und Prüfen bei sehr tief geschachtelten Archiven kann sehr viel Rechnerzeit und -Ressourcen benötigen. Bei aktivierter Option beschränken Sie die Tiefe der Suche in mehrfach gepackten Archiven auf eine bestimmte Zahl an Pack-Ebenen (Maximale Rekursionstiefe). So sparen Sie Zeit- und Rechnerressourcen.

> **Hinweis**
> Um einen Virus bzw. ein unerwünschtes Programm innerhalb eines Archivs zu ermitteln, muss der System-Scanner bis zu der Rekursions-Ebene scannen, in der sich der Virus bzw. das unerwünschte Programm befindet.

Maximale Rekursionstiefe

Um die maximale Rekursionstiefe eingeben zu können, muss die Option **Rekursionstiefe einschränken** aktiviert sein.
Sie können die gewünschte Rekursionstiefe entweder direkt eingeben oder aber mittels der Pfeiltasten rechts vom Eingabefeld ändern. Erlaubte Werte sind 1 bis 99. Der Standardwert ist 20 und wird empfohlen.

Standardwerte

Die Schaltfläche stellt die vordefinierten Werte für die Suche in Archiven wieder her.

Archiv-Liste

In diesem Anzeigebereich können Sie einstellen, welche Archive der System-Scanner durchsuchen soll. Sie müssen hierfür die entsprechenden Einträge markieren.

Ausnahmen

Vom System-Scanner auszulassende Dateiobjekte

Die Liste in diesem Fenster enthält Dateien und Pfade, die bei der Suche nach Viren bzw. unerwünschten Programmen vom System-Scanner nicht berücksichtigt werden sollen.

Bitte tragen Sie hier so wenige Ausnahmen wie möglich und wirklich nur Dateien ein, die aus welchen Gründen auch immer, bei einem normalen Suchlauf nicht geprüft werden sollen. Wir empfehlen, diese Dateien auf jeden Fall auf Viren bzw. unerwünschte Programme zu untersuchen, bevor sie in diese Liste aufgenommen werden!

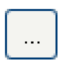
> **Hinweis**
> Die Einträge der Liste dürfen zusammen maximal 6000 Zeichen ergeben.

> **Warnung**
> Diese Dateien werden bei einem Suchlauf nicht berücksichtigt!

> **Hinweis**
> Die in dieser Liste aufgenommenen Dateien werden in der Reportdatei vermerkt. Kontrollieren Sie bitte von Zeit zu Zeit die Reportdatei nach diesen nicht überprüften Dateien, denn vielleicht gibt es den Grund, aus dem Sie eine Datei hier ausgenommen haben gar nicht mehr. Dann sollten Sie den Namen dieser Datei aus der Liste wieder entfernen.

Eingabefeld

In dieses Feld geben Sie den Namen des Dateiobjekts ein, der von der Direktsuche nicht berücksichtigt wird. Standardmäßig ist kein Dateiobjekt eingegeben.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die gewünschte Datei bzw. den gewünschten Pfad auszuwählen.
Haben Sie einen Dateinamen mit vollständigem Pfad eingegeben, wird genau diese Datei nicht auf Befall überprüft. Falls Sie einen Dateinamen ohne Pfad eingetragen haben, wird jede Datei mit diesem Namen (egal in welchem Pfad oder auf welchem Laufwerk) nicht durchsucht.

Hinzufügen

Mit der Schaltfläche können Sie das im Eingabefeld eingegebene Dateiobjekt in das Anzeigefenster übernehmen.

Löschen

Die Schaltfläche löscht einen markierten Eintrag in der Liste. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.

Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Suchengine.

Avira Produkte enthalten sehr leistungsfähige Heuristiken, mit denen unbekannte Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware typisch sind. Erfüllt der untersuchte Code diese charakteristischen Merkmale, wird er als verdächtig gemeldet. Dies bedeutet aber nicht zwingend, dass es sich bei dem Code tatsächlich um Malware handelt; es können auch Fehlmeldungen vorkommen. Die Entscheidung, was mit dem betreffenden Code zu geschehen hat, ist vom Nutzer selbst zu treffen, z.B. an Hand seines Wissens darüber, ob die Quelle, die den gemeldeten Code enthält, vertrauenswürdig ist.

Makrovirenheuristik

Makrovirenheuristik

Ihr Avira Produkt enthält eine sehr leistungsfähige Makrovirenheuristik. Bei aktivierter Option werden bei möglicher Reparatur alle Makros im betroffenen Dokument gelöscht, alternativ werden verdächtige Dokumente nur gemeldet, d.h. Sie erhalten eine Warnung. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Advanced Heuristic Analysis and Detection (AHeAD)

AHeAD aktivieren

Ihr Avira Programm beinhaltet mit der Avira AHeAD-Technologie eine sehr leistungsfähige Heuristik, die auch unbekannte (neue) Malware erkennen kann. Bei aktivierter Option können Sie hier einstellen, wie "scharf" diese Heuristik sein soll. Diese Einstellung ist standardmäßig aktiviert.

Erkennungsstufe niedrig

Bei aktivierter Option wird weniger unbekannte Malware erkannt, die Gefahr von möglichen Fehlerkennungen ist hier gering.

Erkennungsstufe mittel

Bei aktivierter Option wird ein ausgewogener Schutz mit wenigen Fehlermeldungen gewährleistet. Diese Einstellung ist standardmäßig aktiviert, wenn Sie die Anwendung dieser Heuristik gewählt haben.

Erkennungsstufe hoch

Bei aktivierter Option wird bedeutend mehr unbekannte Malware erkannt, mit Fehlmeldungen muss jedoch gerechnet werden.

12.1.2 Report

Der System-Scanner besitzt eine umfangreiche Protokollierfunktion. Damit erhalten Sie exakte Informationen über die Ergebnisse einer Direktsuche. Die Reportdatei enthält alle Einträge des Systems sowie Warnungen und Meldungen der Direktsuche.

> **Hinweis**
> Damit Sie bei einem Fund von Viren oder unerwünschten Programmen nachvollziehen können, welche Aktionen der System-Scanner ausgeführt hat, sollte immer eine Reportdatei erstellt werden.

Protokollierung

Aus

Bei aktivierter Option protokolliert der System-Scanner die Aktionen und Ergebnisse der Direktsuche nicht.

Standard

Bei aktivierter Option protokolliert der System-Scanner die Namen der betroffenen Dateien mit Pfadangabe. Zudem wird die Konfiguration für den aktuellen Suchlauf, Versionsinformationen und Informationen zum Lizenznehmer in die Reportdatei geschrieben.

Erweitert

Bei aktivierter Option protokolliert der System-Scanner zusätzlich zu den Standard-Informationen auch Warnungen und Hinweise. Die Reportdatei zeigt ein "(Cloud)"-Suffix an, um die Warnungen von der Cloud-Sicherheit zu identifizieren.

Vollständig

Bei aktivierter Option protokolliert der System-Scanner zusätzlich alle durchsuchten Dateien. Zudem werden alle betroffenen Dateien sowie Warnungen und Hinweise mit in die Reportdatei aufgenommen.

> **Hinweis**
> Sollten Sie uns einmal eine Reportdatei zusenden müssen (zur Fehlersuche), bitten wir Sie, diese Reportdatei in diesem Modus zu erstellen.

12.2 Echtzeit-Scanner

Die Rubrik Echtzeit-Scanner der Konfiguration ist für die Konfiguration der Echtzeitsuche zuständig.

12.2.1 Suche

Üblicherweise werden Sie Ihr System ständig überwachen wollen. Dafür nutzen Sie den Echtzeit-Scanner (Echtzeitsuche = On-Access-Scanner). Damit können Sie u.a. alle Dateien, die auf dem Computer kopiert oder geöffnet werden, "on the fly", nach Viren und unerwünschten Programmen durchsuchen lassen.

Dateien

Der Echtzeit-Scanner kann einen Filter verwenden, um nur Dateien mit einer bestimmten Endung (Typ) zu prüfen.

Alle Dateien

Bei aktivierter Option werden alle Dateien, unabhängig von ihrem Inhalt und ihrer Dateierweiterung, nach Viren bzw. unerwünschten Programmen durchsucht.

> **Hinweis**
> Ist **Alle Dateien** aktiv, lässt sich die Schaltfläche **Dateierweiterungen** nicht anwählen.

Intelligente Dateiauswahl

Bei aktivierter Option wird die Auswahl der zu prüfenden Dateien vollautomatisch vom Programm übernommen. Dies bedeutet, dass das Programm anhand des Inhalts einer Datei entscheidet, ob diese auf Viren und unerwünschte Programme geprüft werden soll oder nicht. Dieses Verfahren ist etwas langsamer als **Dateierweiterungsliste verwenden**, aber wesentlich sicherer, da nicht nur anhand der Dateierweiterung geprüft wird.

> **Hinweis**
> Ist **Intelligente Dateiauswahl** aktiv, lässt sich die Schaltfläche **Dateierweiterungen** nicht anwählen.

Dateierweiterungsliste verwenden

Bei aktivierter Option werden nur Dateien mit einer vorgegebenen Endung durchsucht. Voreingestellt sind alle Dateitypen, die Viren und unerwünschte Programme enthalten können. Die Liste lässt sich über die Schaltfläche "**Dateierweiterung"** manuell editieren. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

> **Hinweis**
> Ist diese Option aktiv und Sie haben alle Einträge aus der Liste mit Dateiendungen gelöscht, wird dies durch den Text "*Keine Dateierweiterungen*" unterhalb der Schaltfläche **Dateierweiterungen** angezeigt.

Dateierweiterungen

Mit Hilfe dieser Schaltfläche wird ein Dialogfenster aufgerufen, in dem alle Dateiendungen angezeigt werden, die bei einem Suchlauf im Modus "**Dateierweiterungsliste verwenden"** untersucht werden. Bei den Endungen sind Standardeinträge vorgegeben, es lassen sich aber auch Einträge hinzufügen oder entfernen.

> **Hinweis**
> Beachten Sie bitte, dass sich die Dateierweiterungsliste von Version zu Version ändern kann.

Suchmodus

Hier wird der Zeitpunkt für das Prüfen einer Datei festgelegt.

Beim Lesen durchsuchen

Bei aktivierter Option prüft der Echtzeit-Scanner die Dateien, bevor sie von einer Anwendung oder dem Betriebssystem gelesen oder ausgeführt werden.

Beim Schreiben durchsuchen

Bei aktivierter Option prüft der Echtzeit-Scanner eine Datei beim Schreiben. Erst nach diesem Vorgang können Sie wieder auf die Datei zugreifen.

Beim Lesen und Schreiben suchen

Bei aktivierter Option prüft der Echtzeit-Scanner Dateien vor dem Öffnen, Lesen und Ausführen und nach dem Schreiben. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Laufwerke

Netzwerklaufwerke überwachen

Bei aktivierter Option werden Dateien auf Netzlaufwerken (gemappte Laufwerke) wie z.B. Server-Volumes, Peer-Laufwerke, etc. überwacht.

> **Hinweis**
> Um die Leistungsfähigkeit Ihres Rechners nicht zu stark zu beeinträchtigen, sollte die Option **Netzwerklaufwerke überwachen** nur im Ausnahmefall aktiviert werden.

> **Warnung**
> Bei deaktivierter Option werden die Netzlaufwerke **nicht** überwacht. Sie sind nicht mehr vor Viren bzw. unerwünschten Programmen geschützt!

> **Hinweis**
> Wenn Dateien auf Netzlaufwerken ausgeführt werden, werden diese vom Echtzeit-Scanner durchsucht - unabhängig von der Einstellung der Option **Netzwerklaufwerke überwachen**. In einigen Fällen werden Dateien auf Netzlaufwerken beim Öffnen durchsucht, obwohl die Option



Netzwerklaufwerke überwachen deaktiviert ist. Der Grund: Auf diese Dateien wird mit der Berechtigung 'Datei ausführen' zugegriffen. Wenn Sie diese Dateien oder auch ausgeführte Dateien auf Netzlaufwerken von einer Überwachung des Echtzeit-Scanners ausnehmen wollen, tragen Sie die Dateien in die Liste der auszulassenden Dateiobjekte ein (siehe: Ausnahmen).

Caching aktivieren

Bei aktivierter Option werden überwachte Dateien auf Netzlaufwerken im Cache des Echtzeit-Scanners zur Verfügung gestellt. Die Überwachung von Netzlaufwerken ohne Caching-Funktion bietet mehr Sicherheit, ist jedoch weniger performant als die Überwachung von Netzlaufwerken mit Caching-Funktion.

Archive

Archive durchsuchen

Bei aktivierter Option werden Archive durchsucht. Die komprimierten Dateien werden durchsucht, dekomprimiert und noch einmal durchsucht. Standardmäßig ist die Option deaktiviert. Die Archivsuche wird über die Rekursionstiefe, die Anzahl der zu durchsuchenden Dateien und die Archivgröße eingeschränkt. Sie können die maximale Rekursionstiefe, die Anzahl der zu durchsuchenden Dateien und die maximale Archivgröße einstellen.

Hinweis
Die Option ist standardmäßig deaktiviert, da der Prozess sehr viel Rechnerleistung in Anspruch nimmt. Generell wird empfohlen, Archive mit der Direktsuche zu prüfen.

Max. Rekursionstiefe

Bei der Suche in Archiven wendet der Echtzeit-Scanner eine rekursive Suche an: Es werden auch Archive in Archiven entpackt und auf Viren und unerwünschte Programme geprüft. Sie können die Rekursionstiefe festlegen. Der Standardwert für die Rekursionstiefe ist 1 und wird empfohlen: Alle Dateien, die direkt im Hauptarchiv liegen, werden durchsucht.

Max. Anzahl Dateien

Bei der Suche in Archiven wird die Suche auf eine maximale Anzahl von Dateien im Archiv beschränkt. Der Standardwert für die maximale Anzahl zu durchsuchender Dateien ist 10 und wird empfohlen.

Max. Größe (KB)

Bei der Suche in Archiven wird die Suche auf eine maximale, zu entpackende Archivgröße beschränkt. Der Standardwert ist 1000 KB und wird empfohlen.

Aktion bei Fund

Sie können Aktionen festlegen, die der Echtzeit-Scanner ausführen soll, wenn ein Virus oder unerwünschtes Programm gefunden wurde.

Interaktiv

Bei aktivierter Option erscheint bei einem Fund des Echtzeit-Scanners eine Desktop-Benachrichtigung. Sie haben die Möglichkeit, die gefundene Malware zu entfernen oder weitere mögliche Aktionen zur Virenbehandlung über die Schaltfläche "**Details**" abzurufen. Die Aktionen werden in einem Dialogfenster angezeigt. Diese Option ist standardmäßig aktiviert.

Erlaubte Aktionen

Reparieren

Der Echtzeit-Scanner repariert die betroffene Datei, falls dies möglich ist.

Umbenennen

Der Echtzeit-Scanner benennt die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Die Datei kann später repariert und wieder umbenannt werden.

Quarantäne

Der Echtzeit-Scanner verschiebt die Datei in die Quarantäne. Die Datei kann vom Quarantänemanager aus wiederhergestellt werden kann, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden. Je nach Datei stehen im Quarantänemanager noch weitere Auswahlmöglichkeiten zur Verfügung (siehe Quarantänemanager).

Löschen

Die Datei wird gelöscht. Dieser Vorgang ist bedeutend schneller als **Überschreiben und löschen** (siehe unten).

Ignorieren

Der Zugriff auf die Datei wird erlaubt und die Datei wird belassen.

Überschreiben und löschen

Der Echtzeit-Scanner überschreibt die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

> **Warnung**
> Ist der Echtzeit-Scanner auf **Beim Schreiben durchsuchen** eingestellt, wird die betroffene Datei nicht erstellt.

Standard

Mit Hilfe dieser Schaltfläche können Sie die Aktion auswählen, die beim Fund eines Virus im Dialogfenster standardmäßig aktiviert ist. Markieren Sie die Aktion, die standardmäßig aktiviert sein soll, und klicken Sie auf die Schaltfläche "**Standard**".

> **Hinweis**
> Die Aktion **Reparieren** kann nicht als Standard-Aktion ausgewählt werden.

Weitere Informationen finden Sie hier.

Automatisch

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms kein Dialog, in dem eine Aktion ausgewählt werden kann. Der Echtzeit-Scanner reagiert nach den von Ihnen in diesem Abschnitt vorgenommenen Einstellungen.

Datei vor Aktion in Quarantäne kopieren

Bei aktivierter Option erstellt der Echtzeit-Scanner eine Sicherheitskopie (Backup) vor der Durchführung der gewünschten Primären bzw. Sekundären Aktion. Die Sicherheitskopie wird in der Quarantäne aufbewahrt. Sie kann vom Quarantänemanager aus wiederhergestellt werden, wenn sie einen informativen Wert hat. Zudem können Sie die Sicherheitskopie an das Avira Malware Research Center senden. Je nach Objekt stehen im Quarantänemanager noch weitere Auswahlmöglichkeiten zur Verfügung (siehe Quarantänemanager)

Primäre Aktion

Die primäre Aktion, ist die Aktion die ausgeführt wird, wenn der Echtzeit-Scanner einen Virus bzw. ein unerwünschtes Programm findet. Ist die Option "**Reparieren**" gewählt, jedoch eine Reparatur der betroffenen Datei nicht möglich, wird die unter "**Sekundäre Aktion**" gewählte Aktion ausgeführt.

> **Hinweis**
> Die Option **Sekundäre Aktion** ist nur dann auswählbar, wenn unter **Primäre Aktion** die Einstellung **Reparieren** ausgewählt wurde.

Reparieren

Bei aktivierter Option repariert der Echtzeit-Scanner betroffene Dateien automatisch. Wenn der Echtzeit-Scanner eine betroffene Datei nicht reparieren kann, führt es alternativ die unter **Sekundäre Aktion** gewählte Option aus.

> **Hinweis**
> Eine automatische Reparatur wird empfohlen, bedeutet aber, dass der Echtzeit-Scanner Dateien auf dem Computer verändert.

Umbenennen

Bei aktivierter Option benennt der Echtzeit-Scanner die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurück benannt werden.

Quarantäne

Bei aktivierter Option verschiebt der Echtzeit-Scanner die Datei in ein Quarantäneverzeichnis. Die Dateien in diesem Verzeichnis können später repariert oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Löschen

Bei aktivierter Option wird die Datei gelöscht. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

Ignorieren

Bei aktivierter Option wird der Zugriff auf die Datei erlaubt und die Datei belassen.

Warnung
Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Überschreiben und löschen

Bei aktivierter Option überschreibt der Echtzeit-Scanner die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

Zugriff verweigern

Bei aktivierter Option trägt der Echtzeit-Scanner den Fund nur in der Reportdatei ein, wenn die Reportfunktion aktiviert ist. Außerdem schreibt der Echtzeit-Scanner einen Eintrag in das Ereignisprotokoll, wenn diese Option aktiviert ist.

Warnung
Ist der Echtzeit-Scanner auf **Beim Schreiben durchsuchen** eingestellt, wird die betroffene Datei nicht erstellt.

Sekundäre Aktion

Die Option "**Sekundäre Aktion"** ist nur dann auswählbar, wenn unter "**Primäre Aktion"** die Option "**Reparieren**" ausgewählt wurde. Mittels dieser Option kann nun entschieden werden, was mit der betroffenen Datei geschehen soll, wenn diese nicht reparabel ist.

Umbenennen

Bei aktivierter Option benennt der Echtzeit-Scanner die Datei um. Ein direkter Zugriff auf diese Dateien (z.B. durch Doppelklick) ist damit nicht mehr möglich. Dateien können später repariert und zurück benannt werden.



Quarantäne

Bei aktivierter Option verschiebt der Echtzeit-Scanner die Datei in Quarantäne. Die Dateien können später repariert oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Löschen

Bei aktivierter Option wird die Datei gelöscht. Dieser Vorgang ist bedeutend schneller als "überschreiben und löschen".

Ignorieren

Bei aktivierter Option wird der Zugriff auf die Datei erlaubt und die Datei belassen.

Warnung
Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Überschreiben und löschen

Bei aktivierter Option überschreibt der Echtzeit-Scanner die Datei mit einem Standardmuster und löscht sie anschließend. Sie kann nicht wiederhergestellt werden.

Zugriff verweigern

Bei aktivierter Option, wird die betroffene Datei nicht erstellt. Der Echtzeit-Scanner trägt den Fund nur in der Reportdatei ein, wenn die Reportfunktion aktiviert ist. Außerdem schreibt der Echtzeit-Scanner einen Eintrag in das Ereignisprotokoll, wenn diese Option aktiviert ist.

Hinweis
Wenn Sie als primäre oder sekundäre Aktion **Löschen** oder **Überschreiben und löschen** ausgewählt haben, beachten Sie bitte folgendes: Bei heuristischen Treffern werden die betroffenen Dateien nicht gelöscht, sondern in die Quarantäne verschoben.

Weitere Aktionen

Ereignisprotokoll verwenden

Bei aktivierter Option wird bei jedem Fund ein Eintrag in das Windows Ereignisprotokoll geschrieben. Die Ereignisse können in der Windows Ereignisanzeige abgerufen werden. Diese Einstellung ist standardmäßig aktiviert.

Ausnahmen

Mit diesen Optionen können Sie Ausnahme-Objekte für den Echtzeit-Scanner (Echtzeitsuche) konfigurieren. Die entsprechenden Objekte werden dann bei der Echtzeitsuche nicht beachtet. Der Echtzeit-Scanner kann über die Liste der

auszulassenden Prozesse deren Dateizugriffe bei der Echtzeitsuche ignorieren. Dies ist zum Beispiel bei Datenbanken oder Backuplösungen sinnvoll.

Beachten Sie bei der Angabe von auszulassenden Prozessen und Dateiobjekten folgendes: Die Liste wird von oben nach unten abgearbeitet. Je länger die Liste ist, desto mehr Prozessorzeit braucht die Abarbeitung der Liste für jeden Zugriff. Halten Sie deshalb die Listen möglichst klein.

Vom Echtzeit-Scanner auszulassende Prozesse

Alle Dateizugriffe von Prozessen in dieser Liste werden von der Überwachung durch den Echtzeit-Scanner ausgenommen.

Eingabefeld

In dieses Feld geben Sie den Namen des Prozesses ein, der von der Echtzeitsuche nicht berücksichtigt werden soll. Standardmäßig ist kein Prozess eingegeben.

Der angegebene Pfad und der Dateiname des Prozesses dürfen maximal 255 Zeichen enthalten. Sie können bis zu 128 Prozesse eingeben. Die Einträge der Liste dürfen zusammen maximal 6000 Zeichen ergeben.

Bei der Angabe des Prozesses werden Unicode-Zeichen akzeptiert. Sie können daher Prozess- oder Verzeichnisnamen angeben, die Sonderzeichen enthalten.

Laufwerke müssen wie folgt angegeben werden: `[Laufwerksbuchstabe]:\`

Das Zeichen Doppelpunkt (:) darf nur zur Angabe von Laufwerken verwendet werden.

Bei der Angabe des Prozesses können Sie die Platzhalter * (beliebig viele Zeichen) und ? (ein einzelnes Zeichen) verwenden:

```
C:\Programme\Anwendung\anwendung.exe
C:\Programme\Anwendung\anwendun?.exe
C:\Programme\Anwendung\anwend*.exe
C:\Programme\Anwendung\*.exe
```

Um zu vermeiden, dass Prozesse global von der Überwachung des Echtzeit-Scanners ausgenommen werden, sind Angaben ungültig, die ausschließlich aus folgenden Zeichen bestehen: * (Stern), ? (Fragezeichen), / (Slash), \ (Backslash), . (Punkt), : (Doppelpunkt).

Sie haben die Möglichkeit, Prozesse ohne vollständige Pfadangabe von der Überwachung des Echtzeit-Scanners auszunehmen: `anwendung.exe`

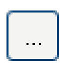
Dies gilt jedoch ausschließlich für Prozesse, deren ausführbare Dateien auf Laufwerken der Festplatte liegen.

Eine vollständige Pfadangabe ist bei Prozessen erforderlich, deren ausführbare Dateien auf verbundenen Laufwerken, z.B. Netzlaufwerken liegen. Beachten Sie hierzu die allgemeinen Hinweise zur Notation von Ausnahmen auf verbundenen Netzlaufwerken.



Geben Sie keine Ausnahmen für Prozesse an, deren ausführbare Dateien auf dynamischen Laufwerken liegen. Dynamische Laufwerke werden für Wechseldatenträger wie CD, DVD oder USB-Stick verwendet.

Warnung
Bitte beachten Sie, dass alle Dateizugriffe, die von Prozessen initiiert werden und die in der Liste vermerkt wurden, von der Suche nach Viren und unerwünschten Programmen ausgeschlossen sind!



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, eine ausführbare Datei auszuwählen.

Prozesse

Die Schaltfläche "**Prozesse"** öffnet das Fenster "*Prozessauswahl*", in dem die laufenden Prozesse angezeigt werden.

Hinzufügen

Mit der Schaltfläche können Sie den im Eingabefeld eingegebenen Prozess in das Anzeigefenster übernehmen.

Löschen

Mit der Schaltfläche entfernen Sie einen markierten Prozess aus dem Anzeigefenster.

Vom Echtzeit-Scanner auszulassende Dateiobjekte

Alle Dateizugriffe auf Objekte in dieser Liste werden von der Überwachung durch den Echtzeit-Scanner ausgenommen.

Eingabefeld

In dieses Feld geben Sie den Namen des Dateiobjekts ein, welches von der Echtzeitsuche nicht berücksichtigt wird. Standardmäßig ist kein Dateiobjekt eingegeben.

Die Einträge der Liste dürfen zusammen nicht mehr als 6000 Zeichen ergeben.

Bei der Angabe von auszulassenden Dateiobjekten können Sie die Platzhalter * (beliebig viele Zeichen) und ? (ein einzelnes Zeichen) verwenden. Es können auch einzelne Dateierweiterungen ausgenommen werden (inklusive Platzhalter):

```
C:\Verzeichnis\*.mdb
*.mdb
*.md?
*.xls*
C:\Verzeichnis\*.log
```

Verzeichnisnamen müssen mit einem Backslash \ abgeschlossen sein.



Wenn ein Verzeichnis ausgenommen wird, werden automatisch auch alle darunter liegende Verzeichnisse mit ausgenommen.

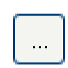
Pro Laufwerk können Sie maximal 20 Ausnahmen mit vollständigem Pfad (beginnend mit dem Laufwerksbuchstaben) angeben.

Bsp.: `C:\Programme\Anwendung\Name.log`

Die maximale Anzahl von Ausnahmen ohne vollständigen Pfad beträgt 64. Bsp:

```
*.log
 \Rechner1\C\Verzeichnis1
```

Bei dynamischen Laufwerken, die als Verzeichnis auf einem anderen Laufwerk eingebunden (gemountet) werden, müssen Sie den Aliasnamen des Betriebssystems für das eingebundene Laufwerk in der Liste der Ausnahmen verwenden:
z.B. `\Device\HarddiskDmVolumes\PhysicalDmVolumes\BlockVolume1\`
Verwenden Sie den Bereitstellungspunkt (mount point) selbst, z.B. `C:\DynDrive`, wird das dynamische Laufwerk trotzdem durchsucht. Sie können den zu verwendenden Aliasnamen des Betriebssystems aus der Report-Datei des Echtzeit-Scanners ermitteln.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, das gewünschte auszulassende Dateiobjekt auszuwählen.

Hinzufügen

Mit der Schaltfläche können Sie das im Eingabefeld eingegebene Dateiobjekt in das Anzeigefenster übernehmen.

Löschen

Mit der Schaltfläche Löschen entfernen Sie ein markiertes Dateiobjekt aus dem Anzeigefenster.

Beachten Sie bei der Angabe von Ausnahmen die weiteren Hinweise

Um Objekte auch dann auszunehmen, wenn darauf mit kurzen DOS-Dateinamen (DOS-Namenskonvention 8.3) zugegriffen wird, muss der entsprechende kurze Dateiname ebenfalls in die Liste eingetragen werden.

Ein Dateiname, der Platzhalter enthält, darf nicht mit einem Backslash abgeschlossen werden.
Beispielsweise:
`C:\Programme\Anwendung\anwend*.exe\`
Dieser Eintrag ist nicht gültig und wird nicht als Ausnahme behandelt!

Beachten Sie bei **Ausnahmen auf verbundenen Netzlaufwerken** folgendes: Wenn Sie den Laufwerksbuchstaben des verbundenen Netzlaufwerks verwenden, werden die angegebenen Dateien und Verzeichnisse NICHT von der Suche des Echtzeit-Scanners



ausgenommen. Wenn der UNC-Pfad in der Liste der Ausnahmen vom UNC-Pfad, der zur Verbindung mit dem Netzlaufwerk genutzt wird, abweicht (Angabe von IP-Adresse in Liste der Ausnahmen - Angabe vom Computername zur Verbindung mit Netzlaufwerk) werden die angegebenen Verzeichnisse und Dateien NICHT von der Suche des Echtzeit-Scanners ausgenommen. Ermitteln Sie den zu verwendenden UNC-Pfad anhand der Report-Datei des Echtzeit-Scanners:
`\\<Computername>\<Freigabe>\` - ODER- `\\<IP-Adresse>\<Freigabe>\`

Anhand der Report-Datei des Echtzeit-Scanners können Sie die Pfade ermitteln, die der Echtzeit-Scanner bei der Suche nach betroffenen Dateien verwendet. Verwenden Sie grundsätzlich in der Liste der Ausnahmen dieselben Pfade. Gehen Sie wie folgt vor: Setzen Sie die Protokoll-Funktion des Echtzeit-Scanners in der Konfiguration unter Report auf **Vollständig**. Greifen Sie nun mit dem aktivierten Echtzeit-Scanner auf die Dateien, Verzeichnisse, eingebundenen Laufwerke oder verbundenen Netzlaufwerke zu. Sie können nun den zu verwendenden Pfad aus der Reportdatei des Echtzeit-Scanners auslesen. Die Reportdatei rufen Sie im Control Center unter Echtzeit-Scanner ab.

Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Suchengine.

Avira Produkte enthalten sehr leistungsfähige Heuristiken, mit denen unbekannte Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware typisch sind. Erfüllt der untersuchte Code diese charakteristischen Merkmale, wird er als verdächtig gemeldet. Dies bedeutet aber nicht zwingend, dass es sich bei dem Code tatsächlich um Malware handelt; es können auch Fehlmeldungen vorkommen. Die Entscheidung, was mit dem betreffenden Code zu geschehen hat, ist vom Nutzer selbst zu treffen, z.B. an Hand seines Wissens darüber, ob die Quelle, die den gemeldeten Code enthält, vertrauenswürdig ist.

Makrovirenheuristik

Makrovirenheuristik

Ihr Avira Produkt enthält eine sehr leistungsfähige Makrovirenheuristik. Bei aktivierter Option werden bei möglicher Reparatur alle Makros im betroffenen Dokument gelöscht, alternativ werden verdächtige Dokumente nur gemeldet, d.h. Sie erhalten eine Warnung. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Advanced Heuristic Analysis and Detection (AHeAD)

AHeAD aktivieren

Ihr Avira Programm beinhaltet mit der Avira AHeAD-Technologie eine sehr leistungsfähige Heuristik, die auch unbekannte (neue) Malware erkennen kann. Bei aktivierter Option können Sie hier einstellen, wie "scharf" diese Heuristik sein soll. Diese Einstellung ist standardmäßig aktiviert.

Erkennungsstufe niedrig

Bei aktivierter Option wird weniger unbekannte Malware erkannt, die Gefahr von möglichen Fehlerkennungen ist hier gering.

Erkennungsstufe mittel

Bei aktivierter Option wird ein ausgewogener Schutz mit wenigen Fehlermeldungen gewährleistet. Diese Einstellung ist standardmäßig aktiviert, wenn Sie die Anwendung dieser Heuristik gewählt haben.

Erkennungsstufe hoch

Bei aktivierter Option wird bedeutend mehr unbekannte Malware erkannt, mit Fehlmeldungen muss jedoch gerechnet werden.

12.2.2 Report

Der Echtzeit-Scanner besitzt eine umfangreiche Protokollierfunktion, die dem Benutzer bzw. dem Administrator exakte Hinweise über die Art und Weise eines Funds geben kann.

Protokollierung

In dieser Gruppe wird der inhaltliche Umfang der Reportdatei festgelegt.

Aus

Bei aktivierter Option erstellt der Echtzeit-Scanner kein Protokoll.
Verzichten Sie nur in Ausnahmefällen auf die Protokollierung, beispielsweise nur dann, wenn Sie Testläufe mit vielen Viren oder unerwünschten Programmen durchführen.

Standard

Bei aktivierter Option nimmt der Echtzeit-Scanner wichtige Informationen (zu Fund, Warnungen und Fehlern) in die Reportdatei auf, weniger wichtige Informationen werden zur besseren Übersicht ignoriert. Diese Einstellung ist standardmäßig aktiviert.

Erweitert

Bei aktivierter Option nimmt der Echtzeit-Scanner auch weniger wichtige Informationen in die Reportdatei mit auf.

Vollständig

Bei aktivierter Option nimmt der Echtzeit-Scanner sämtliche Informationen - auch solche zu Dateigröße, Dateityp, Datum etc. - in die Reportdatei auf.

Reportdatei beschränken



Größe beschränken auf n MB

Bei aktivierter Option lässt sich die Reportdatei auf eine bestimmte Größe beschränken; mögliche Werte: 1 bis 100 MB. Bei der Beschränkung der Reportdatei wird ein Spielraum von etwa 50 Kilobytes eingeräumt, um die Belastung des Rechners niedrig zu halten. Übersteigt die Größe der Protokolldatei die angegebene Größe um 50 Kilobytes, werden automatisch so lange alte Einträge gelöscht, bis die angegebene Größe weniger 50 Kilobytes erreicht worden ist.

Reportdatei vor dem Kürzen sichern

Bei aktivierter Option wird die Reportdatei vor dem Kürzen gesichert.

Konfiguration in Reportdatei schreiben

Bei aktivierter Option wird die verwendete Konfiguration der Echtzeitsuche in die Reportdatei geschrieben.

Hinweis
Wenn Sie keine Beschränkung der Reportdatei angegeben haben, wird automatisch eine neue Reportdatei angelegt, wenn die Reportdatei eine Größe von 100 MB erreicht hat. Es wird eine Sicherung der alten Reportdatei angelegt. Es werden bis zu drei Sicherungen alter Reportdateien vorgehalten. Die jeweils ältesten Sicherungen werden gelöscht.

12.3 Update

Unter der Rubrik **Update** konfigurieren Sie die automatische Ausführung von Updates. Sie haben die Möglichkeit, verschiedene Update-Intervalle einzustellen.

Automatisches Update

alle n Tag(e) / Stunde(n) / Minute(n)

In diesem Feld können Sie das Intervall angeben, in dem automatische Updates ausgeführt werden sollen. Um das Update-Intervall zu ändern, markieren Sie eine der Zeitangaben im Feld und ändern Sie diese über die Pfeiltasten rechts vom Eingabefeld.

Auftrag zusätzlich bei Internet Verbindung starten

Bei aktivierter Option wird der Update-Auftrag zusätzlich zum festgelegten Update-Intervall bei jedem Zustandekommen einer Internet-Verbindung durchgeführt.

Auftrag nachholen, wenn die Zeit bereits abgelaufen ist

Bei aktivierter Option werden Update-Aufträge durchgeführt, die in der Vergangenheit liegen und zum gewünschten Zeitpunkt nicht durchgeführt werden konnten, beispielsweise bei ausgeschaltetem Computer.

12.3.1 Webserver

Webserver

Das Update kann direkt über einen Webserver im Internet durchgeführt werden.

Verbindung zum Webserver

Vorhandene Verbindung (Netzwerk) verwenden

Diese Einstellung wird angezeigt, wenn Ihre Verbindung über ein Netzwerk verwendet wird.

Die folgende Verbindung verwenden

Diese Einstellung wird angezeigt, wenn Sie Ihre Verbindung individuell definieren.

Der Updater erkennt automatisch, welche Verbindungsoptionen vorhanden sind. Nicht vorhandene Verbindungsoptionen sind grau hinterlegt und können nicht aktiviert werden. Eine DFÜ-Verbindung können Sie z.B. manuell über einen Telefonbucheintrag in Windows herstellen.

Benutzer

Geben Sie den Benutzernamen Ihres ausgewählten Kontos ein.

Kennwort

Geben Sie das Kennwort für dieses Konto ein. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt.

> **Hinweis**
> Wenden Sie sich an den Internetdienstanbieter, wenn Sie den Benutzernamen oder das Kennwort eines vorhandenen Internetkontos vergessen haben.

> **Hinweis**
> Die automatische Einwahl des Updaters über sogenannte Dial-Up Tools (z.B. SmartSurfer, Oleco, ...) steht momentan noch nicht zur Verfügung.

Eine für das Update geöffnete DFÜ-Verbindung wieder beenden

Bei aktivierter Option wird die für das Update geöffnete DFÜ-Verbindung automatisch wieder unterbrochen, sobald der Download erfolgreich durchgeführt wurde.

> **Hinweis**
> Die Option ist nur unter Windows XP verfügbar. Ab Windows Vista wird die DFÜ-Verbindung, die für das Update geöffnet wurde, immer beendet, sobald der Download durchgeführt wurde.

Proxy Einstellungen

Proxyserver

Keinen Proxyserver verwenden

Bei aktivierter Option erfolgt Ihre Verbindung zum Webserver nicht über einen Proxyserver.

Windows Systemeinstellungen verwenden

Bei aktivierter Option werden die aktuellen Windows Systemeinstellungen für die Verbindung zum Webserver über einen Proxyserver verwendet. Sie konfigurieren die Windows Systemeinstellungen zur Verwendung eines Proxyservers unter **Systemsteuerung > Internetoptionen > Verbindungen > LAN-Einstellungen**. Im Internet Explorer können Sie im Menü **Extras** ebenfalls auf die Internetoptionen zugreifen.

Warnung
Wenn Sie einen Proxyserver nutzen, der eine Authentifizierung erfordert, geben Sie die Daten unter der Option **Verbindung über diesen Proxy** vollständig an. Die Option **Windows Systemeinstellungen verwenden** kann nur für Proxyserver ohne Authentifizierung genutzt werden.

Verbindung über diesen Proxyserver

Bei aktivierter Option erfolgt Ihre Verbindung zum Webserver über einen Proxyserver, wobei die von Ihnen angegebenen Einstellungen verwendet werden.

Adresse

Geben Sie den Rechnernamen oder die IP-Adresse des Proxyservers ein, den Sie für die Verbindung mit dem Webserver verwenden möchten.

Port

Geben Sie die Port-Nummer des Proxyservers ein, den Sie für die Verbindung mit dem Webserver verwenden möchten.

Login Name

Geben Sie einen Benutzernamen für die Anmeldung am Proxyserver ein.

Login Kennwort

Geben Sie das entsprechende Kennwort für die Anmeldung am Proxyserver ein. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt.

Beispiele:

Adresse: `proxy.domain.de` Port: `8080`

Adresse: `192.168.1.100` Port: `3128`



12.4 Backup

Unter **Konfiguration > Internet Sicherheit > Backup** können Sie die Komponente Backup konfigurieren.

12.4.1 Einstellungen

Unter **Einstellungen** können Sie das Verhalten der Backup-Komponente konfigurieren.

Nur geänderte Dateien sichern

Bei aktivierter Option wird ein inkrementelles Backup erstellt: Es werden nur die Dateien im Backup-Profil gesichert, die seit der letzten Datensicherung geändert wurden. Bei deaktivierter Option wird bei jeder Sicherung eines Backup-Profils ein Voll-Backup erstellt: Es werden alle Dateien im Backup-Profil gesichert. Diese Option ist standardmäßig aktiviert und wird empfohlen, da inkrementelle Backups schneller und ressourcenschonender erstellt werden können als Volldatensicherungen.

Vor dem Sichern auf Malware prüfen

Bei aktivierter Option werden beim Backup die zu sichernden Dateien auf Viren und Malware geprüft. Betroffene Dateien werden nicht gesichert. Diese Option ist standardmäßig aktiviert und wird empfohlen.

12.4.2 Ausnahmen

Unter **Ausnahmen** können Sie festlegen, welche Dateiobjekte und Dateitypen bei einem Backup gesichert bzw. nicht gesichert werden sollen.

Vom Backup auszulassende Dateiobjekte

Die Liste in diesem Fenster enthält Dateien und Pfade, die bei einem Backup nicht gesichert werden sollen.

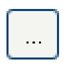
> **Hinweis**
> Die Einträge der Liste dürfen zusammen maximal 6000 Zeichen ergeben.

> **Hinweis**
> Die in dieser Liste aufgenommenen Dateien werden in der Reportdatei vermerkt.



Eingabefeld

In dieses Feld geben Sie den Namen des Dateiobjekts ein, das nicht gesichert werden soll. Standardmäßig ist der Pfad zum temporären Verzeichnis für lokale Einstellungen des angemeldeten Benutzers eingegeben.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die gewünschte Datei bzw. den gewünschten Pfad auszuwählen.
Haben Sie einen Dateinamen mit vollständigem Pfad eingegeben, wird genau diese Datei nicht mitgesichert. Falls Sie einen Dateinamen ohne Pfad eingetragen haben, wird jede Datei mit diesem Namen (egal in welchem Pfad oder auf welchem Laufwerk) nicht gesichert.

Hinzufügen

Mit der Schaltfläche können Sie das im Eingabefeld eingegebene Dateiobjekt in das Anzeigefenster übernehmen.

Löschen

Die Schaltfläche löscht einen markierten Eintrag in der Liste. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.

Liste zurücksetzen

Diese Schaltfläche stellt die vordefinierten Standardwerte wieder her.

Beachten Sie folgende Punkte

- Die Platzhalter * (beliebig viele Zeichen) und ? (ein einzelnes Zeichen) sind nur in Dateinamen erlaubt.
- Die Liste wird von oben nach unten abgearbeitet.
- Wenn ein Verzeichnis ausgenommen wird, werden automatisch auch alle darunter liegende Verzeichnisse mit ausgenommen.
- Es können auch einzelne Dateierweiterungen ausgenommen werden (inklusive Platzhalter).
- Um Objekte auch dann auszunehmen, wenn darauf mit kurzen DOS-Dateinamen (DOS-Namenskonvention 8.3) zugegriffen wird, muss der entsprechende kurze Dateiname ebenfalls in die Liste eingetragen werden.

Hinweis
Ein Dateiname, der Platzhalter enthält, darf nicht mit einem Backslash abgeschlossen werden. Beispielsweise:
`C:\Programme\Anwendung\anwend*.exe\`
Dieser Eintrag ist nicht gültig und wird nicht als Ausnahme behandelt!



Beispiele

- `anwendung.exe`
- `\Programme\`
- `C:\*.*`
- `C:\*`
- `*.exe`
- `*.xl?`
- `*.*`
- `C:\Programme\Anwendung\anwendung.exe`
- `C:\Programme\Anwendung\anwend*.exe`
- `C:\Programme\Anwendung\anwend*`
- `C:\Programme\Anwendung\anwend????.e*`
- `C:\Programme\`
- `C:\Programme`
- `C:\Programme\Anwendung\*.mdb`

Dateierweiterungslisten

Alle Dateierweiterungen berücksichtigen

Bei aktivierter Option werden alle Dateien im Backup-Profil gesichert.

Liste der auszulassenden Dateierweiterungen aktivieren

Bei aktivierter Option werden alle Dateien im Backup-Profil gesichert mit Ausnahme der Dateien, deren Dateierweiterungen in die Liste der auszulassenden Dateierweiterungen eingetragen wurden.

Dateierweiterungen

Mit Hilfe dieser Schaltfläche wird ein Dialogfenster aufgerufen, in dem alle Dateiendungen angezeigt werden, die bei einem Backup mit aktivierter Option "**Liste der auszulassenden Dateierweiterungen aktivieren**" nicht gesichert werden. Bei den Endungen sind Standardeinträge vorgegeben, es lassen sich aber auch Einträge hinzufügen oder entfernen.

Liste der einzubeziehenden Dateierweiterungen aktivieren

Bei aktivierter Option werden nur die Dateien gesichert, deren Dateierweiterungen in die Liste der zu beachtenden Dateierweiterungen eingetragen wurden.

Dateierweiterungen

Mit Hilfe dieser Schaltfläche wird ein Dialogfenster aufgerufen, in dem alle Dateiendungen angezeigt werden, die bei einem Backup mit aktivierter Option "**Liste der einzubeziehenden Dateierweiterungen aktivieren**" gesichert werden. Bei den Endungen sind Standardeinträge vorgegeben, es lassen sich aber auch Einträge hinzufügen oder entfernen.

12.4.3 Report

Die Backup-Komponente besitzt eine umfangreiche Protokollierfunktion.

Protokollierung

In dieser Gruppe wird der inhaltliche Umfang der Reportdatei festgelegt.

Aus

Bei aktivierter Option erstellt die Backup-Komponente kein Protokoll. Verzichten Sie nur in Ausnahmefällen auf die Protokollierung.

Standard

Bei aktivierter Option nimmt die Backup-Komponente wichtige Informationen (zur Sicherung, zu Virenfunden, Warnungen und Fehlern) in die Reportdatei auf, weniger wichtige Informationen werden zur besseren Übersicht ignoriert. Diese Einstellung ist standardmäßig aktiviert.

Erweitert

Bei aktivierter Option nimmt die Backup-Komponente auch weniger wichtige Informationen in die Reportdatei mit auf.

Vollständig

Bei aktivierter Option nimmt die Backup-Komponente sämtliche Informationen zum Backup-Verlauf und zur Virensuche in die Reportdatei auf.

12.5 FireWall

Avira Internet Security ermöglicht Ihnen, die Avira FireWall zu konfigurieren:

- Avira FireWall

12.5.1 Avira FireWall

Die Rubrik **FireWall** unter **Konfiguration > Internet Sicherheit** ist für die Konfiguration der Avira FireWall in Betriebssystemen bis Windows 7 zuständig.

Adapterregeln

Als Adapter wird in der Avira FireWall jede von einer Software simulierte Hardwareeinheit (z.B. Miniport, Bridge Connection, usw.) oder jede Hardwareeinheit (z.B. eine Netzwerkkarte) betrachtet.

Die Avira FireWall zeigt die Adapterregeln für alle auf Ihrem Computer existierenden Adapter an, für die ein Treiber installiert ist.



- ICMP-Protokoll
- TCP Port-Scan
- UDP Port-Scan
- Eingehende Regeln
- Ausgehende Regeln
- Schaltflächen

Eine vordefinierte Adapterregel ist abhängig vom Sicherheitsniveau. Sie können das *Sicherheitsniveau* über die Rubrik **Internet Sicherheit > FireWall** des Control Center ändern oder die Adapterregeln auf Ihre Bedürfnisse anpassen. Haben Sie die Adapterregeln auf Ihre Bedürfnisse angepasst, wird unter der Rubrik FireWall des Control Center im Bereich *Sicherheitsniveau* der Regler auf **Benutzer** platziert.

> **Hinweis**
> Die Standardeinstellung des Sicherheitsniveaus für alle vordefinierten Regeln der Avira FireWall ist **Mittel**.

ICMP-Protokoll

Das Internet Control Message Protocol (ICMP) dient in Netzwerken zum Austausch von Fehler- und Informationsmeldungen. Das Protokoll wird auch für Statusmeldungen mittels Ping oder Tracert verwendet.
Mit dieser Regel können Sie ein- und ausgehende ICMP-Typen definieren, die blockiert werden sollen, die Parameter für Flooding festlegen und das Verhalten bei Vorliegen von fragmentierten ICMP-Paketen definieren. Diese Regel dient dazu sogenannte ICPM Flood-Attacken zu verhindern, die zu einer Belastung bzw. Überlastung des Prozessors des attackierten Rechners führen können, da auf jedes Paket geantwortet wird.

Vordefinierte Regeln für das ICMP-Protokoll

Einstellung	Regeln
Niedrig	Blockiert eingehende Typen: **kein Typ**. Blockiert ausgehende Typen: **kein Typ**. Flooding vermuten, wenn die Verzögerung zwischen Paketen weniger als **50** Millisekunden beträgt. Fragmentierte ICMP-Pakete **ablehnen**.
Mittel	Dieselben Regeln wie bei der Einstellung *Niedrig*.

Hoch	Blockiert eingehende Typen: **verschiedene Typen**. Blockiert ausgehende Typen: **verschiedene Typen**. Flooding vermuten, wenn die Verzögerung zwischen Paketen weniger als **50** Millisekunden beträgt. Fragmentierte ICMP-Pakete **ablehnen**.

Blockierte eingehende Typen: keine Typen/ verschiedene Typen

Mit einem Klick auf den Link öffnen Sie eine Liste mit ICMP-Pakettypen. Aus dieser Liste können Sie die gewünschten eingehenden ICMP-Nachrichtentypen, die Sie blockieren möchten, auswählen.

Blockierte ausgehende Typen: keine Typen/ verschiedene Typen

Mit einem Klick auf den Link öffnen Sie eine Liste mit ICMP-Pakettypen. Aus dieser Liste können Sie die gewünschten ausgehenden ICMP-Nachrichtentypen, die Sie blockieren möchten, auswählen.

Flooding vermuten

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie den Maximalwert für die erlaubte ICMP-Verzögerung eintragen können.

Fragmentierte ICMP-Pakete

Mit einem Klick auf den Link haben Sie die Möglichkeit zwischen "**ablehnen**" und "**nicht ablehnen**" von fragmentierten ICMP Paketen zu wählen.

TCP Port-Scan

Mit dieser Regel können Sie definieren, wann die FireWall von einem TCP Port-Scan ausgehen und wie sie sich in einem solchen Fall verhalten soll. Diese Regel dient dazu, sogenannte TCP Port-Scan Attacken zu verhindern, über die offene Ports auf Ihrem Computer festgestellt werden können. Angriffe dieser Art werden meist wiederum dazu benutzt, Schwachstellen Ihres Computers auszunutzen, über die möglicherweise weitaus gefährlichere Attacken ausgeführt werden können.

Vordefinierte Regeln für den TCP Port-Scan

Einstellung	Regeln
Niedrig	TCP Port-Scan vermuten, wenn **50** oder mehr Ports in **5000** Millisekunden gescannt worden sind. Bei Feststellung eines TCP Port-Scans, IP-Adresse des Angreifers **in Ereignisdatenbank schreiben** und den Regeln **nicht hinzufügen**, um den Angriff zu blockieren.
Mittel	TCP Port-Scan vermuten, wenn **50** oder mehr Ports in **5000** Millisekunden gescannt worden sind. Bei Feststellung eines TCP Port-Scans, IP-Adresse des Angreifers **in Ereignisdatenbank schreiben** und den Regeln **hinzufügen**, um den Angriff zu blockieren.
Hoch	Dieselben Regeln wie bei der Einstellung *Mittel*.

Ports

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die Anzahl der Ports eintragen können, die gescannt worden sein müssen, damit von einem TCP Port-Scan ausgegangen wird.

Port-Scan Zeitfenster

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie das Zeitintervall eintragen können, in dem eine bestimmte Anzahl von Ports gescannt worden sein müssen, damit von einem TCP Port-Scan ausgegangen wird.

Ereignisdatenbank

Mit einem Klick auf diesen Link haben Sie die Möglichkeit zu entscheiden, ob die IP-Adresse des Angreifers in die Ereignisdatenbank geschrieben werden soll oder nicht.

Regel

Mit einem Klick auf diesen Link haben Sie die Möglichkeit zu entscheiden, ob die Regel zur Blockierung des TCP Port-Scan Angriffs hinzugefügt werden soll oder nicht.

UDP Port-Scan

Mit dieser Regel definieren Sie, wann die FireWall von einem UDP Port-Scan ausgehen und wie sie sich in einem solchen Fall verhalten soll. Diese Regel dient dazu sogenannte UDP Port-Scan Attacken zu verhindern, über die offene Ports auf Ihrem Computer festgestellt werden können. Angriffe dieser Art werden meist wiederum dazu benutzt, Schwachstellen Ihres Computers auszunutzen, über die möglicherweise weitaus gefährlichere Attacken ausgeführt werden können.

Vordefinierte Regeln für den UDP Port-Scan



Einstellung	Regeln
Niedrig	UDP Port-Scan vermuten, wenn **50** oder mehr Ports in **5000** Millisekunden gescannt worden sind. Bei Feststellung eines UDP Port-Scans, IP-Adresse des Angreifers **in Ereignisdatenbank schreiben** und den Regeln **nicht hinzufügen**, um den Angriff zu blockieren.
Mittel	UDP Port-Scan vermuten, wenn **50** oder mehr Ports in **5000** Millisekunden gescannt worden sind. Bei Feststellung eines TCP Port-Scans, IP-Adresse des Angreifers **in Ereignisdatenbank schreiben** und den Regeln **hinzufügen**, um den Angriff zu blockieren.
Hoch	Dieselbe Regel wie bei der Einstellung *Mittel*.

Ports

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie Anzahl der Ports eintragen können, die gescannt worden sein müssen, damit von einem UDP Port-Scan ausgegangen wird.

Port-Scan Zeitfenster

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie das Zeitintervall eintragen können, in dem eine bestimmte Anzahl von Ports gescannt worden sein müssen, damit von einem UDP Port-Scan ausgegangen wird.

Ereignisdatenbank

Mit einem Klick auf diesen Link haben Sie die Möglichkeit zu entscheiden, ob die IP-Adresse des Angreifers in die Ereignisdatenbank geschrieben werden soll oder nicht.

Regel

Mit einem Klick auf diesen Link haben Sie die Möglichkeit zu entscheiden, ob die Regel zur Blockierung des UDP Port-Scan Angriffs hinzugefügt werden soll oder nicht.

Eingehende Regeln

Eingehende Regeln dienen zur Kontrolle des eingehenden Datenverkehrs durch die Avira FireWall.

Warnung
Da bei der Filterung eines Paketes die entsprechenden Regeln nacheinander angewendet werden, ist deren Reihenfolge von besonderer Bedeutung. Bitte



ändern Sie die Reihenfolge der Regeln nur dann, wenn Sie sich ganz sicher sind, was Sie damit bewirken.

Vordefinierte Regeln zur Überwachung des TCP-Datenverkehrs



Einstellung	Regeln
Niedrig	Eingehender Datenverkehr wird von der Avira FireWall nicht blockiert.
Mittel	• **Bestehende TCP-Verbindung auf Port 135 zulassen** TCP-Pakete **Erlauben**, von Adresse **0.0.0.0** mit Maske **0.0.0.0**, wenn der lokale Port in **{135}** und der remote Port in **{0-65535}** liegen. Anwenden auf **Pakete von vorhandenen Verbindungen**. **Nicht in Ereignisdatenbank schreiben**, wenn das Paket der Regel entspricht. Erweitert: Pakete auswählen, die folgende Bytes **<leer>** mit Maske **<leer>** bei Offset **0** haben. • **TCP-Pakete auf Port 135 zurückweisen** TCP-Pakete **Ablehnen**, von Adresse **0.0.0.0** mit Maske **0.0.0.0**, wenn der lokale Port in **{135}** und der remote Port in **{0-65535}** liegen. Anwenden auf **alle Pakete**. **Nicht in Ereignisdatenbank schreiben**, wenn das Paket der Regel entspricht. Erweitert: Pakete auswählen, die folgende Bytes **<leer>** mit Maske **<leer>** bei Offset **0** haben. • **Überwachen des TCP konformen Datenverkehrs** TCP-Pakete **Erlauben**, von Adresse **0.0.0.0** mit Maske **0.0.0.0**, wenn der lokale Port in **{0-65535}** und der remote Port in **{0-65535}** liegen. Anwenden auf **Beginn des Verbindungsaufbaus und auf Pakete von vorhandenen Verbindungen**. **Nicht in Ereignisdatenbank schreiben**, wenn das Paket der Regel entspricht. Erweitert: Pakete auswählen, die folgende Bytes **<leer>** mit Maske **<leer>** bei Offset **0** haben. • **Alle TCP-Pakete zurückweisen** TCP-Pakete **Ablehnen**, von Adresse **0.0.0.0** mit Maske **0.0.0.0**, wenn der lokale Port in **{0-65535}** und der remote Port in **{0-65535}** liegen. Anwenden auf **alle Pakete**. **Nicht in Ereignisdatenbank schreiben**, wenn das Paket der Regel entspricht. Erweitert: Pakete auswählen, die folgende Bytes **<leer>** mit Maske **<leer>** bei Offset **0** haben.



Hoch	**Zugelassenen TCP-Datenverkehr überwachen** TCP-Pakete **Erlauben**, von Adresse **0.0.0.0** mit Maske **0.0.0.0**, wenn der lokale Port in **{0-65535}** und der remote Port in **{0-65535}** liegen. Anwenden auf **Pakete von vorhandenen Verbindungen**. **Nicht in Ereignisdatenbank schreiben**, wenn das Paket der Regel entspricht. Erweitert: Pakete auswählen, die folgende Bytes **<leer>** mit Maske **<leer>** bei Offset **0** haben.

TCP-Pakete erlauben / ablehnen

Mit einem Klick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte TCP-Pakete zulassen oder zurückweisen wollen.

IP-Adresse

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die gewünschte IPv4- oder IPv6-Adresse eintragen können.

IP-Maske

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die gewünschte IPv4- oder IPv6-Maske eintragen können.

Lokale Ports

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie einen oder mehrere gewünschte lokale Ports und auch ganze Portbereiche eintragen können.

Remote Ports

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie einen oder mehrere gewünschte Remote Ports und auch ganze Portbereiche eintragen können.

Anwendungsmethode

Mit einem Klick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie die Regel auf Pakete von vorhandenen Verbindungen anwenden möchten, auf den Beginn des Verbindungsaufbaus und Pakete von vorhandenen Verbindungen oder auf alle Verbindungen.

Ereignisdatenbank

Mit einem Klick auf den Link haben Sie die Möglichkeit zu entscheiden, in die Ereignisdatenbank zu schreiben oder nicht, wenn das Paket der Regel entspricht.

Erweitert

Die Option **Erweitert** erlaubt eine Filterung aufgrund des Inhaltes. So können Sie zum Beispiel Pakete ablehnen, die spezifische Daten mit einem bestimmten Offset

enthalten. Wenn Sie diese Option nicht nutzen möchten, dann wählen Sie keine oder eine leere Datei aus.

Filterung nach Inhalt: Bytes

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die Datei auswählen können, die den speziellen Buffer enthält.

Filterung nach Inhalt: Maske

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die spezielle Maske auswählen können.

Filterung nach Inhalt: Offset

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie den Offset für die inhaltliche Filterung angeben können. Der Offset wird vom Ende des TCP-Headers an berechnet.

Vordefinierte Regeln zur Überwachung des UDP-Datenverkehrs

Einstellung	Regeln
Niedrig	-
Mittel	• **Überwachen des UDP konformen Datenverkehrs** UDP-Pakete **Erlauben**, von Adresse **0.0.0.0** mit Maske **0.0.0.0**, wenn der lokale Port in **{0-65535}** und der remote Port in **{0-65535}** liegen. Regel anwenden auf **geöffnete Ports** für **alle Datenströme**. **Nicht in Ereignisdatenbank schreiben**, wenn das Paket der Regel entspricht. Erweitert: Pakete auswählen, die folgende Bytes **<leer>** mit Maske **<leer>** bei Offset **0** haben. • **Alle UDP-Pakete zurückweisen** UDP-Pakete **Ablehnen**, von Adresse **0.0.0.0** mit Maske **0.0.0.0**, wenn der lokale Port in **{0-65535}** und der remote Port in **{0-65535}** liegen. Anwenden auf **alle Ports** für **alle Datenströme**. **Nicht in Ereignisdatenbank schreiben**, wenn das Paket der Regel entspricht. Erweitert: Pakete auswählen, die folgende Bytes **<leer>** mit Maske **<leer>** bei Offset **0** haben.

Hoch	**Zugelassenen UDP-Datenverkehr überwachen** UDP-Pakete **Erlauben**, von Adresse **0.0.0.0** mit Maske **0.0.0.0**, wenn der lokale Port in **{0-65535}** und der remote Port in **{53, 67, 68, 88,...}** liegen. Regel anwenden auf **geöffnete Ports** für **alle Datenströme**. **Nicht in Ereignisdatenbank schreiben**, wenn das Paket der Regel entspricht. Erweitert: Pakete auswählen, die folgende Bytes **<leer>** mit Maske **<leer>** bei Offset **0** haben.

UDP-Pakete erlauben / ablehnen

Mit einem Klick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte UDP-Pakete zulassen oder zurückweisen wollen.

IP-Adresse

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die gewünschte IPv4- oder IPv6-Adresse eintragen können.

IP-Maske

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die gewünschte IPv4- oder IPv6-Maske eintragen können.

Lokale Ports

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie einen oder mehrere gewünschte lokale Ports und auch ganze Portbereiche eintragen können.

Remote Ports

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie einen oder mehrere gewünschte Remote Ports und auch ganze Portbereiche eintragen können.

Anwendungsmethode

Ports

Mit einem Klick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie die Regel auf alle Ports oder nur auf alle geöffnete Ports anwenden möchten.

Datenströme

Mit einem Klick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie die Regel auf alle Datenströme oder nur ausgehende Datenströme anwenden möchten.

Ereignisdatenbank

Mit einem Klick auf den Link haben Sie die Möglichkeit zu entscheiden, in die Ereignisdatenbank zu schreiben oder nicht, wenn das Paket der Regel entspricht.



Erweitert

Die Option **Erweitert** erlaubt eine Filterung aufgrund des Inhaltes. So können Sie zum Beispiel Pakete ablehnen, die spezifische Daten mit einem bestimmten Offset enthalten. Wenn Sie diese Option nicht nutzen möchten, dann wählen Sie keine oder eine leere Datei aus.

Filterung nach Inhalt: Bytes

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die Datei auswählen können, die den speziellen Buffer enthält.

Filterung nach Inhalt: Maske

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die spezielle Maske auswählen können.

Filterung nach Inhalt: Offset

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie den Offset für die inhaltliche Filterung angeben können. Der Offset wird vom Ende des UDP-Headers an berechnet.

Vordefinierte Regeln zur Überwachung des ICMP-Datenverkehrs

Einstellung	Regeln
Niedrig	-
Mittel	**Keine ICMP-Pakete auf der Basis der IP-Adresse verwerfen** ICMP-Pakete **Erlauben** von Adresse **0.0.0.0** mit Maske **0.0.0.0**. **Nicht in Ereignisdatenbank schreiben**, wenn das Paket der Regel entspricht. Erweitert: Pakete auswählen, die folgende Bytes **<leer>** mit Maske **<leer>** bei Offset **0** haben.
Hoch	Dieselbe Regel wie bei der Einstellung *Mittel*.

ICMP-Pakete erlauben / ablehnen

Mit einem Klick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte ICMP-Pakete zulassen oder zurückweisen wollen.

IP-Adresse

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die gewünschte IPv4-Adresse eintragen können.



IP-Maske

Mit einem Klick auf diesen Link öffnen Sie ein Dialogfenster, in dem Sie die gewünschte IPv4-Maske eintragen können.

Ereignisdatenbank

Mit einem Klick auf den Link haben Sie die Möglichkeit zu entscheiden, in eine Ereignisdatenbank zu schreiben oder nicht, wenn das Paket der Regel entspricht.

Erweitert

Die Option **Erweitert** erlaubt eine Filterung aufgrund des Inhaltes. So können Sie zum Beispiel Pakete ablehnen, die spezifische Daten mit einem bestimmten Offset enthalten. Wenn Sie diese Option nicht nutzen möchten, dann wählen Sie keine oder eine leere Datei aus.

Filterung nach Inhalt: Bytes

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die Datei auswählen können, die den speziellen Buffer enthält.

Filterung nach Inhalt: Maske

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die spezielle Maske auswählen können.

Filterung nach Inhalt: Offset

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie den Offset für die inhaltliche Filterung angeben können. Der Offset wird vom Ende des ICMP-Headers an berechnet.

Vordefinierte Regel für IP-Pakete

Einstellung	Regeln
Niedrig	-
Mittel	-
Hoch	**Alle IP-Pakete zurückweisen** **Ablehnen IPv4**- Pakete von Adresse **0.0.0.0** mit Maske **0.0.0.0**. **Nicht in Ereignisdatenbank schreiben**, wenn das Paket der Regel entspricht.

Erlauben /Ablehnen

Mit einem Klick auf den Link haben Sie die Möglichkeit zu entscheiden, ob Sie speziell definierte IP-Pakete zulassen oder zurückweisen wollen.



IPv4 / IPv6

Mit einem Klick auf den Link wählen Sie zwischen IPv4 und IPv6.

IP-Adresse

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die gewünschte IPv4- oder IPv6-Adresse eintragen können.

IP-Maske

Mit einem Klick auf den Link öffnen Sie ein Dialogfenster, in dem Sie die gewünschte IPv4- oder IPv6-Maske eintragen können.

Ereignisdatenbank

Mit einem Klick auf den Link haben Sie die Möglichkeit zu entscheiden, in die Ereignisdatenbank zu schreiben oder nicht, wenn das Paket der Regel entspricht.

Ausgehende Regeln

Ausgehende Regeln dienen zur Kontrolle des ausgehenden Datenverkehrs durch die Avira FireWall. Sie können eine ausgehende Regel für die folgenden Protokolle definieren: IP, ICMP, UDP und TCP.

Warnung
Da bei der Filterung eines Paketes die entsprechenden Regeln nacheinander angewendet werden, ist deren Reihenfolge von besonderer Bedeutung. Bitte ändern Sie die Reihenfolge der Regeln nur dann, wenn Sie sich ganz sicher sind, was Sie damit bewirken.

Schaltflächen

Schaltfläche	Beschreibung
Hinzufügen	Ermöglicht Ihnen das Erstellen einer neuen Regel. Wenn Sie auf diese Schaltfläche klicken, erscheint das Dialogfenster "Neue Regel hinzufügen". In diesem Dialogfenster können Sie neue Regeln auswählen.
Entfernen	Entfernen einer ausgewählten Regel.
Nach oben	Verschieben einer ausgewählten Regel um eine Position nach oben, wodurch die Priorität dieser Regel erhöht wird.
Nach unten	Verschieben einer ausgewählten Regel um eine Position nach unten, wodurch die Priorität dieser Regel reduziert wird.

Umbenennen	Umbenennen einer ausgewählten Regel.

Hinweis
Sie können neue Regeln für einzelne Adapter oder aber für alle vorhandenen Adapter des Computers hinzufügen. Um eine Adapterregel für alle Adapter hinzuzufügen, wählen Sie **Arbeitsplatz** in der angezeigten Adapterstruktur und klicken Sie auf die Schaltfläche **Hinzufügen**. Siehe Neue Regel hinzufügen.

Hinweis
Um die Position einer Regel zu ändern, können Sie die Regel auch mit der Maus an die gewünschte Position ziehen.

Neue Regel hinzufügen

In diesem Fenster können Sie neue eingehende und ausgehende Regeln auswählen. Die ausgewählte Regel wird mit Standard-Angaben ins Fenster **Adapterregeln** übernommen und kann dort weiter spezifiziert werden. Neben eingehenden und ausgehenden Regeln stehen Ihnen weitere Regeln zur Verfügung.

Mögliche Regeln

Peer-To-Peer Netzwerk erlauben

Erlaubt Peer-To-Peer Verbindungen: Eingehende TCP-Kommunikation auf Port 4662 und eingehende UDP-Kommunikation auf Port 4672

TCP-Port

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den erlaubten TCP-Port eingeben können.

UDP-Port

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den erlaubten UDP-Port eingeben können.

VMWARE-Verbindungen erlauben

Erlaubt die Kommunikation zwischen VMWare-Systemen

IP-Adresse blockieren

Blockiert den gesamten Verkehr von einer bestimmten IP-Adresse

IP-Version

Mit einem Klick auf den Link wählen Sie zwischen IPv4 und IPv6.



IP-Adresse

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IPv4- oder IPv6--Adresse eingeben können.

Subnetz blockieren

Blockiert den gesamten Verkehr von einer bestimmten IP-Adresse und Subnetzmaske

IP-Version

Mit einem Klick auf den Link wählen Sie zwischen IPv4 und IPv6.

IP-Adresse

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eingeben können.

Subnetzmaske

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte Subnetzmaske eingeben können.

IP-Adresse erlauben

Erlaubt den gesamten Verkehr von einer bestimmten IP-Adresse

IP-Version

Mit einem Klick auf den Link wählen Sie zwischen IPv4 und IPv6.

IP-Adresse

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eingeben können.

Subnetz erlauben

Erlaubt den gesamten Verkehr von einer bestimmten IP-Adresse und Subnetzmaske

IP-Version

Mit einem Klick auf den Link wählen Sie zwischen IPv4 und IPv6.

IP-Adresse

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eingeben können.

Subnetzmaske

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte Subnetzmaske eingeben können.

Web-Server erlauben

Erlaubt die Kommunikation von einem Web-Server auf Port 80: Eingehende TCP-Kommunikation auf Port 80



Port

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den vom Webserver genutzten Port eingeben können.

VPN-Verbindungen erlauben

Erlaubt VPN-Verbindungen (Virtual Private Network) mit einer bestimmten IP: Eingehender UDP-Datenverkehr auf x Ports, eingehender TCP-Datenverkehr auf x Ports, eingehender IP-Datenverkehr mit den Protokollen ESP(50), GRE (47)

IP-Version

Mit einem Klick auf den Link wählen Sie zwischen IPv4 und IPv6.

IP-Adresse

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eingeben können.

"Remote Desktop" Verbindung erlauben

Erlaubt "Remote-Desktop" Verbindungen (Remote Desktop Protocol) auf Port 3389

Port

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den Port, der für die erlaubte Remote-Desktop-Verbindung genutzt wird, eingeben können.

VNC-Verbindung erlauben

Erlaubt VNC-Verbindungen (Virtual Network Computing) auf Port 5900

Port

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den Port, der für die erlaubte VNC-Verbindung genutzt wird, eingeben können.

Datei- und Druckerfreigaben erlauben

Erlaubt Zugriff auf Drucker- und Dateifreigaben: Eingehender TCP-Datenverkehr auf Port 137, 139 und eingehender UDP-Datenverkehr auf Port 445 von einer beliebigen IP-Adresse.

Mögliche eingehende Regeln

- **Eingehende IP-Regel**
- **Eingehende ICMP-Regel**
- **Eingehende UDP-Regel**
- **Eingehende TCP-Regel**
- **Eingehende IP-Protokollregel**

Mögliche ausgehende Regeln

- **Ausgehende IP-Regel**

- **Ausgehende ICMP-Regel**
- **Ausgehende UDP-Regel**
- **Ausgehende TCP-Regel**
- **Ausgehende IP-Protokollregel**

> **Hinweis**
> Die Optionen bei den möglichen eingehenden Regeln und den ausgehenden Regeln sind identisch mit den Optionen der vordefinierten Regeln der entsprechenden Protokolle, wie unter FireWall > Adapterregeln beschrieben.

Schaltflächen

Schaltfläche	Beschreibung
OK	Die markierte Regel wird als neue Adapterregel übernommen.
Abbrechen	Das Fenster wird geschlossen, ohne eine neue Regel hinzuzufügen.

Anwendungsregeln

Anwendungsregeln für den Benutzer

Diese Liste enthält alle Anwender im System. Falls Sie als Administrator angemeldet sind, können Sie einen Benutzer auswählen, für den Sie Regeln erstellen möchten. Falls Sie kein Anwender mit privilegierten Rechten sind, zeigt Ihnen die Liste nur den aktuell angemeldeten Benutzer.

Anwendung

Diese Tabelle zeigt Ihnen die Liste der Anwendungen, für die Regeln definiert sind. Die Liste zeigt die Einstellungen für jede Anwendung, die seit der Installation der Avira FireWall ausgeführt wurde und für die eine Regel gespeichert wurde.

Standardansicht

Spalte	Beschreibung
Anwendung	Name der Anwendung
Aktive Verbindungen	Anzahl der von der Anwendung geöffneten aktiven Verbindungen
Aktion	Zeigt die Aktion an, die die Avira FireWall automatisch durchführen wird, falls die Anwendung das Netzwerk nutzt, gleich welcher Art diese Nutzung ist. Durch einen Mausklick auf den Link haben Sie die Möglichkeit, auf eine andere Aktionsart zu wechseln. Die Aktionsarten **Fragen**, **Erlauben** oder **Ablehnen** stehen zur Auswahl. Die Standardeinstellung ist **Fragen.**

Erweiterte Konfiguration

Wenn Sie die Netzwerkzugänge einer Anwendung individuell regeln möchten, können Sie vergleichbar den Adapterregeln spezifizierte Anwendungsregeln, die auf Paketfiltern basieren, erstellen.

- Ändern Sie unter **Konfiguration > Internet Sicherheit > FireWall > Einstellungen** die Einstellung für *Anwendungsregeln*: Aktivieren Sie die Option **Erweiterte Einstellungen** und speichern Sie die Einstellung mit **Übernehmen** oder **OK**.
  - ↳ Es wird nun unter **Konfiguration > Internet Sicherheit > FireWall > Anwendungsregeln** in der Liste der Anwendungsregeln eine weitere Spalte **Filterung** mit dem Eintrag **Einfach** angezeigt.

Spalte	Beschreibung
Anwendung	Name der Anwendung.
Aktive Verbindungen	Anzahl der von der Anwendung geöffneten aktiven Verbindungen



Aktion	Zeigt die Aktion an, die die Avira FireWall automatisch durchführen wird, falls die Anwendung das Netzwerk nutzt, gleich welcher Art diese Nutzung ist. Bei der Einstellung **Filterung - Einfach** können Sie durch einen Mausklick auf den Link auf eine andere Aktionsart zu wechseln. Die Aktionsarten **Fragen**, **Erlauben,** und **Ablehnen** stehen zur Auswahl. Bei der Einstellung **Filterung - Erweitert** wird die Aktionsart **Regeln** angezeigt. Der Link **Regeln** öffnet das Fenster **Erweiterte Anwendungsregeln**, in dem Sie spezifizierte Regeln für die Anwendung hinterlegen können.
Filterung	Zeigt die Art der Filterung an. Durch einen Mausklick auf den Link haben Sie die Möglichkeit, auf eine andere Filterung zu wechseln. **Einfach**: Bei einfacher Filterung wird die angegeben Aktion bei allen Netzwerkaktivitäten der Software-Anwendung ausgeführt. **Erweitert**: Bei der Filterung werden die Regeln ausgeführt, die in der erweiterten Konfiguration hinterlegt wurden.

- Wenn Sie für eine Anwendung spezifizierte Anwendungsregeln erstellen möchten, wechseln Sie unter **Filterung** auf den Eintrag **Erweitert**.
  - ↳ In der Spalte **Aktion** wird nun der Eintrag **Regeln** angezeigt.
- Klicken Sie auf **Regeln**, um in das Fenster zur Erstellung von spezifizierten Anwendungsregeln zu gelangen.

Spezifizierte Anwendungsregeln in der erweiterten Konfiguration

Mit spezifizierten Anwendungsregeln können Sie spezifizierten Datenverkehr der Anwendung zulassen oder zurückweisen sowie das passive Abhören von einzelnen Ports zulassen oder zurückweisen. Sie haben folgende Optionen:

Code-Injektion ablehnen/ erlauben

Code-Injektion ist eine Technik, mit der man Code im Adressraum eines anderen Prozesses zur Ausführung bringt, indem man diesen Prozess zwingt, eine Dynamic Link Library (DLL) zu laden. Die Technik der Code-Injektion wird u.a. von Malware eingesetzt, um Code unter dem Deckmantel eines anderen Programms auszuführen. Dadurch können z.B. Zugriffe auf das Internet vor der Avira FireWall verschleiert werden. Standardmäßig wird Code-Injektion für alle signierten Anwendungen erlaubt.

Passives Abhören der Anwendung von Ports zulassen oder zurückweisen

Datenverkehr zulassen oder zurückweisen:

Eingehende und / oder ausgehende IP-Pakete zulassen oder zurückweisen

Eingehende und / oder ausgehende TCP-Pakete zulassen oder zurückweisen

Eingehende und / oder ausgehende UDP-Pakete zulassen oder zurückweisen

Sie können zu jeder Anwendung beliebig viele Anwendungsregeln erstellen. Die Anwendungsregeln werden in der angezeigten Reihenfolge ausgeführt (Weitere Informationen finden Sie unter Erweiterte Anwendungsregeln).

> **Hinweis**
> Wenn Sie die Filterung von **Erweitert** nach **Einfach** bei einer Anwendungsregel ändern, werden die bereits angelegten Anwendungsregeln in der erweiterten Konfiguration nicht endgültig gelöscht, sondern nur deaktiviert. Wechseln Sie wieder zur Filterung **Erweitert**, werden die bereits angelegten Anwendungsregeln wieder aktiviert und im Fenster der erweiterten Konfiguration für **Anwendungsregeln** angezeigt.

Anwendungsdetails

In dieser Rubrik werden Detailinformationen zu der Anwendung angezeigt, die Sie in der Liste der Anwendungen ausgewählt haben.

- *Name* - Name der Anwendung.
- *Pfad* - Pfad zur ausführbaren Datei der Anwendung.

Schaltflächen

Schaltfläche	Beschreibung
Anwendung hinzufügen	Ermöglicht Ihnen das Erstellen einer neuen Anwendungsregel. Wenn Sie auf diese Schaltfläche klicken, erscheint ein Dialogfenster. Nun können Sie eine Anwendung auswählen, für die Sie eine Regel erstellen möchten.
Regel entfernen	Entfernen der ausgewählten Anwendungsregel.



Details einblenden	Im Fenster *Eigenschaften* werden Detailinformationen zu der Anwendung angezeigt, die Sie in der Liste ausgewählt haben.
Neu laden	Erneutes Laden der Liste der Anwendungen mit gleichzeitigem Verwerfen aller gerade gemachten Änderungen an den Anwendungsregeln.

Erweiterte Anwendungsregeln

In dem Fenster **Erweiterte Anwendungsregeln** haben Sie die Möglichkeit, spezifizierte Regeln für den Datenverkehr von Anwendungen und das Abhören von Ports zu erstellen. Sie erstellen eine neue Regel mit der Schaltfläche **Hinzufügen**. Im unteren Fensterbereich können Sie die Regel weiter spezifizieren. Zu einer Anwendung können Sie beliebig viele Regeln erstellen. Die Regeln werden in der angezeigten Reihenfolge ausgeführt. Sie können mit den Schaltflächen **Nach oben** und **Nach unten** die Reihenfolge der Regeln ändern.

> **Hinweis**
> Um die Position einer Anwendungsregel zu ändern, können Sie die Regel auch mit der Maus an die gewünschte Position ziehen.

Anwendungsdetails

Im Bereich Anwendungsdetails werden Informationen zur ausgewählten Anwendung angezeigt:

- *Name* - Name der Anwendung.
- *Pfad* - Pfad zur ausführbaren Datei der Anwendung.

Regeloptionen

Code-Injektion ablehnen/ erlauben

Durch Mausklick auf den Link können Sie festlegen, ob Sie die Code-Injektion bei der ausgewählten Anwendung zurückweisen oder zulassen

Regeltyp: Verkehr / Abhören

Durch Mausklick auf den Link können Sie festlegen, ob Sie eine Regel zum Datenverkehr oder zum Abhören von Ports erstellen.

Aktion: Erlauben/ Ablehnen

Durch Mausklick auf den Link können Sie festlegen, welche Aktion mit der Regel ausgeführt wird.

Port

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie den lokalen Port eingeben können, auf den sich die Abhör-Regel bezieht. Sie können auch mehrere Ports oder Portbereiche eingeben.

Ausgehende, eingehende, alle Pakete

Durch Mausklick auf den Link können Sie festlegen, ob die Verkehr-Regel alle Pakete, nur die ausgehenden oder nur die eingehenden Pakete überwacht.

IP-Pakete / TCP-Pakete / UDP-Pakete

Durch Mausklick auf den Link, können Sie festlegen, welches Protokoll die Verkehr-Regel überwacht.

Optionen für IP-Pakete

IP-Adresse

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Adresse eingeben können.

IP-Maske

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte IP-Maske eingeben können.

Optionen für TCP-Pakete/ UDP-Pakete

Lokale IP-Adresse

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte lokale IP-Adresse eingeben können.

Lokale IP-Maske

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte lokale IP-Maske eingeben können.

Remote IP-Adresse

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte remote IP-Adresse eingeben können.

Remote IP-Maske

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie die gewünschte remote IP-Maske eingeben können.

Lokaler Port

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie einen oder mehrere gewünschte lokale Ports oder auch ganze Portbereiche eintragen können.



Remote Port

Durch Mausklick auf den Link öffnet sich ein Dialogfenster, in dem Sie einen oder mehrere gewünschte remote Ports oder auch ganze Portbereiche eintragen können.

Nicht in Reportdatei schreiben / In Reportdatei schreiben

Durch Mausklick auf den Link können Sie festlegen, ob bei einer Regelentsprechung ein Eintrag in die Reportdatei vom Programm vorgenommen wird.

Schaltflächen

Schaltfläche	Beschreibung
Hinzufügen	Es wird eine neue Anwendungsregel erstellt.
Entfernen	Die ausgewählte Anwendungsregel wird gelöscht.
Nach oben	Die ausgewählte Anwendungsregel wird um eine Position nach oben verschoben, wodurch die Priorität der Regel erhöht wird.
Nach unten	Die ausgewählte Anwendungsregel wird um eine Position nach unten verschoben, wodurch die Priorität der Regel reduziert wird.
Umbenennen	Die ausgewählte Regel wird editiert, so dass ein neuer Regelname eingegeben werden kann.
Anwenden	Die vorgenommenen Änderungen werden übernommen und durch die Avira FireWall direkt angewendet.

OK	Die vorgenommenen Änderungen werden übernommen. Das Fenster zur Konfiguration der Anwendungsregeln wird geschlossen.
Abbrechen	Das Fenster zur Konfiguration der Anwendungsregeln wird geschlossen ohne die vorgenommenen Änderungen zu übernehmen.

Vertrauenswürdige Anbieter

Unter *Vertrauenswürdige Anbieter* wird eine Liste von vertrauenswürdigen Software-Herstellern angezeigt.

Sie können Hersteller aus der Liste entfernen oder hinzufügen, indem Sie die Option **Diesem Anbieter immer vertrauen** im Popup-Fenster **Netzwerkereignis** nutzen. Sie können den Netzzugriff von Anwendungen, die von den aufgelisteten Anbietern signiert sind, standardmäßig erlauben, indem Sie die Option **Von vertrauenswürdigen Anbietern erstellte Anwendungen automatisch zulassen** aktivieren.

Vertrauenswürdige Anbieter für Benutzer

Diese Liste enthält alle Benutzer im System. Falls Sie als Administrator angemeldet sind, können Sie einen Benutzer auswählen, dessen Liste vertrauenswürdiger Anbieter Sie einsehen oder pflegen möchten. Falls Sie kein Benutzer mit privilegierten Rechten sind, zeigt Ihnen die Liste nur den aktuell angemeldeten Benutzer.

Von vertrauenswürdigen Anbietern erstellte Anwendungen automatisch zulassen

Bei aktivierter Option wird Anwendungen mit einer Signatur von bekannten und vertrauenswürdigen Anbietern automatisch der Zugang zum Netzwerk erlaubt. Die Option ist standardmäßig aktiviert.

Anbieter

Die Liste zeigt alle Anbieter, die als vertrauenswürdig eingestuft werden.

Schaltflächen

Schaltfläche	Beschreibung
Entfernen	Der markierte Eintrag wird aus der Liste der vertrauenswürdigen Anbieter entfernt. Um den ausgewählten Anbieter endgültig aus der Liste zu entfernen, klicken Sie auf **Übernehmen** oder **OK** im Fenster der Konfiguration.
Neu laden	Die vorgenommenen Änderungen werden rückgängig gemacht: Die letzte gespeicherte Liste wird geladen.

> **Hinweis**
> Wenn Sie Anbieter aus der Liste entfernen und anschließend die Schaltfläche **Übernehmen** klicken, werden die Anbieter endgültig aus der Liste gelöscht. Die Änderung kann nicht mit **Neu laden** rückgängig gemacht werden. Sie haben jedoch die Möglichkeit, über die Option **Diesem Anbieter immer vertrauen** im Popup-Fenster **Netzwerkereignis** einen Anbieter wieder zur Liste der vertrauenswürdigen Anbieter hinzuzufügen.

> **Hinweis**
> Die Avira FireWall priorisiert Anwendungsregeln vor den Einträgen in der Liste der vertrauenswürdigen Anbieter: Wenn Sie eine Anwendungsregel erstellt haben und der Anbieter der Anwendung ist in der Liste der vertrauenswürdigen Anbieter aufgeführt, wird die Anwendungsregel ausgeführt.

Einstellungen

Erweiterte Einstellungen

Windows-Firewall beim Hochfahren deaktivieren

Bei aktivierter Option ist die Windows-Firewall beim Hochfahren des Rechners deaktiviert. Diese Option ist standardmäßig aktiviert.

Zeitüberschreitung der Regel

Immer blockieren

Bei aktivierter Option wird eine Regel, die beispielsweise bei einem Port-Scan automatisch erstellt wurde, beibehalten.

Regel entfernen nach n Sekunden

Bei aktivierter Option wird eine Regel, die beispielsweise bei einem Portscan automatisch erstellt wurde, nach der von Ihnen angegebenen Zeit wieder entfernt. Diese Option ist standardmäßig aktiviert. In diesem Feld können Sie die Sekunden-Anzahl angeben, nach der die Regel entfernt wird.

Benachrichtigungen

Unter Benachrichtigungen legen Sie fest, bei welchen Ereignissen Sie eine Desktopbenachrichtigung der Avira FireWall erhalten möchten.

Port Scan

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn von der Avira FireWall ein Port Scan erkannt wurde.

Flooding

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn von der Avira FireWall eine Flooding-Attacke erkannt wurde.

Anwendungen gesperrt

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn die Avira FireWall eine Netzwerkaktivität einer Anwendung zurückgewiesen, d.h. blockiert hat.

IP gesperrt

Bei aktivierter Option erhalten Sie eine Desktopbenachrichtigung, wenn die Avira FireWall den Datenverkehr von einer IP-Adresse zurückgewiesen hat.

Anwendungsregeln

Mit den Optionen im Bereich Anwendungsregeln stellen Sie die Konfigurationsmöglichkeiten für Anwendungsregeln unter der Rubrik FireWall > Anwendungsregeln ein.

Erweiterte Einstellungen

Bei aktivierter Option haben Sie die Möglichkeit, verschiedene Netzwerkzugänge einer Anwendung individuell zu regeln.

Grundeinstellungen

Bei aktivierter Option kann nur eine einzige Aktion für verschiedene Netzwerkzugänge der Anwendung eingestellt werden.

Popup-Einstellungen

Popup-Einstellungen



Startblock des Prozesses überprüfen

Bei aktivierter Option erfolgt eine präzisere Überprüfung des Prozess Stapels. Die Avira FireWall geht dann davon aus, dass jeder Prozess im Stapel, der nicht vertrauenswürdig ist, derjenige ist, über dessen Kindprozess auf das Netzwerk zugegriffen wird. Deshalb wird in diesem Fall für jeden nicht vertrauenswürdigen Prozess im Stapel ein eigenes Popup-Fenster geöffnet. Diese Option ist standardmäßig deaktiviert.

Mehrere Dialogfenster pro Prozess anzeigen

Bei aktivierter Option wird jedes Mal, wenn eine Anwendung versucht eine Netzwerkverbindung herzustellen, ein Popup-Fenster geöffnet. Alternativ erfolgt die Information nur beim ersten Verbindungsversuch. Diese Option ist standardmäßig deaktiviert.

Aktion für diese Anwendung speichern

Immer aktiviert

Bei aktivierter Option ist die Option "**Aktion für diese Anwendung speichern**" des Dialogfensters "**Netzwerkereignis**" standardmäßig aktiviert.

Immer deaktiviert

Bei aktivierter Option ist die Option "**Aktion für diese Anwendung speichern**" des Dialogfensters "**Netzwerkereignis**" standardmäßig deaktiviert.

Signierte Anwendungen erlauben

Bei aktivierter Option ist beim Netzzugriff signierter Anwendungen bestimmter Hersteller die Option "**Aktion für diese Anwendung speichern**" des Dialogfensters "**Netzwerkereignis**" automatisch aktiviert. Diese signierten Anwendungen werden von sogenannten "Vertrauenswürdigen Anbietern" zur Verfügung gestellt (siehe Vertrauenswürdige Anbieter).

Letzten Stand merken

Bei aktivierter Option wird die Aktivierung der Option "**Aktion für diese Anwendung speichern**" des Dialogfensters "**Netzwerkereignis**" gehandhabt wie beim letzten Netzwerkereignis. Wurde beim letzten Netzwerkereignis die Option "**Aktion für diese Anwendung speichern**" aktiviert, ist die Option beim folgenden Netzwerkereignis aktiv. Wurde beim letzten Netzwerkereignis die Option "**Aktion für diese Anwendung speichern"** deaktiviert, ist die Option beim folgenden Netzwerkereignis deaktiviert.

Details anzeigen

In dieser Gruppe von Konfigurationsoptionen können Sie die Anzeige von Detailinformationen im Fenster **Netzwerkereignis** einstellen.



Details auf Anfrage anzeigen

Bei aktivierter Option werden die Detailinformationen im Fenster "**Netzwerkereignis**" nur auf Anfrage angezeigt, d.h. eine Anzeige der Detailinformationen erfolgt mit Klick auf die Schaltfläche "**Details einblenden**" im Fenster "**Netzwerkereignis**".

Details immer anzeigen

Bei aktivierter Option werden die Detailinformationen im Fenster "**Netzwerkereignis**" immer angezeigt.

Letzten Stand merken

Bei aktivierter Option wird die Anzeige von Detailinformationen gehandhabt wie beim vorangegangenen Netzwerkereignis. Wurden beim letzten Netzwerkereignis Detailinformationen angezeigt oder abgerufen, werden beim folgenden Netzwerkereignis Detailinformationen angezeigt. Wurden beim letzten Netzwerkereignis die Detailinformationen nicht angezeigt oder ausgeblendet, werden beim folgenden Netzwerkereignis die Detailinformationen nicht angezeigt.

12.6 Browser-Schutz

Die Rubrik **Browser-Schutz** unter **Konfiguration > Internet Sicherheit** ist für die Konfiguration des Browser-Schutzes zuständig.

12.6.1 Suche

Mit dem Browser-Schutz schützen Sie sich vor Viren und Malware, die über Webseiten auf Ihren Computer gelangen, die Sie aus dem Internet in Ihren Webbrowser laden. In der Rubrik **Suche** können Sie das Verhalten des Browser-Schutzes einstellen.

Suche

IPv6 Unterstützung

Bei aktivierter Option wird die Internet-Protokoll-Version 6 vom Browser-Schutz unterstützt. Diese Option ist für Neu- oder Änderungsinstallationen unter Windows 8 nicht verfügbar.

Drive-By Schutz

Unter *Drive-By Schutz* haben Sie die Möglichkeit, Einstellungen zum Blockieren von I-Frames, auch Inlineframes genannt, vorzunehmen. I-Frames sind HTML-Elemente, d.h. Elemente von Internetseiten, die einen Bereich einer Webseite abgrenzen. Mit I-Frames können andere Webinhalte - meist anderer URLs - als selbständige Dokumente in einem Unterfenster des Browsers geladen und angezeigt werden. Meist werden I-Frames für Banner-Werbung genutzt. In einigen Fällen werden I-Frames zum Verstecken von Malware verwendet. In diesen Fällen ist der Bereich des I-Frame im Browser meist kaum oder nicht sichtbar. Mit der Option **Verdächtige I-Frames blockieren** haben Sie die Möglichkeit, das Laden von I-Frames zu kontrollieren und zu blockieren.



Verdächtige I-Frames blockieren

Bei aktivierter Option werden I-Frames auf angeforderten Webseiten nach bestimmten Kriterien geprüft. Sind auf einer angeforderten Webseite verdächtige I-Frames vorhanden, wird das I-Frame blockiert. Im Fenster des I-Frames wird eine Fehlermeldung angezeigt.

Aktion bei Fund

Sie können Aktionen festlegen, die der Browser-Schutz ausführen soll, wenn ein Virus oder unerwünschtes Programm gefunden wurde.

Interaktiv

Bei aktivierter Option erscheint während der Direktsuche bei einem Fund eines Virus bzw. unerwünschten Programms ein Dialogfenster, in dem Sie auswählen können, was mit der betroffenen Datei weiter geschehen soll. Diese Einstellung ist standardmäßig aktiviert.

Fortschrittsbalken anzeigen

Bei aktivierter Option erscheint eine Desktopbenachrichtigung mit einem Download-Fortschrittsbalken, wenn ein Download oder das Herunterladen von Webseiten-Inhalten ein Timeout von 20 Sek. überschreitet. Diese Desktopbenachrichtigung dient insbesondere zur Kontrolle beim Herunterladen von Webseiten mit größerem Datenvolumen: Beim Surfen mit Browser-Schutz werden die Webseiteninhalte im Internet-Browser nicht sukzessive geladen, da sie vor der Anzeige im Internet-Browser nach Viren und Marlware durchsucht werden. Diese Option ist standardmäßig deaktiviert.

Weitere Informationen finden Sie hier.

Automatisch

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms kein Dialog, in dem eine Aktion ausgewählt werden kann. Der Browser-Schutz reagiert nach den von Ihnen in diesem Abschnitt vorgenommenen Einstellungen.

Primäre Aktion

Die primäre Aktion ist die Aktion, die ausgeführt wird, wenn der Browser-Schutz einen Virus bzw. ein unerwünschtes Programm findet.

Zugriff verweigern

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden nicht an Ihren Webbrowser gesendet. Im Webbrowser wird eine Fehlermeldung zur Zugriffsverweigerung angezeigt. Der Browser-Schutz trägt den Fund in die Reportdatei ein, vorausgesetzt die Reportfunktion ist aktiviert.

In Quarantäne verschieben

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden beim Fund eines Virus bzw. einer Malware in die Quarantäne verschoben. Die

betroffene Datei kann vom Quarantänemanager aus wiederhergestellt werden, wenn sie einen informativen Wert hat oder - falls nötig - an das Avira Malware Research Center geschickt werden.

Ignorieren

Die vom Webserver angeforderte Webseite bzw. die übertragenen Daten und Dateien werden vom Browser-Schutz an Ihren Webbrowser weitergeleitet. Der Zugriff auf die Datei wird erlaubt und die Datei wird belassen.

Warnung
Die betroffene Datei bleibt auf Ihrem Computer aktiv! Es kann ein erheblicher Schaden auf Ihrem Computer verursacht werden!

Gesperrte Zugriffe

Unter **Gesperrte Zugriffe** können Sie Dateitypen und MIME-Typen (Inhaltstypen der übertragenen Daten) angeben, die vom Browser-Schutz blockiert werden sollen. Mit dem Web-Filter können Sie bekannte, unerwünschte URLs, wie z.B. Phishing- und Malware-URLs, blockieren. Der Browser-Schutz verhindert die Übertragung der Daten vom Internet auf Ihr Computersystem.

Vom Browser-Schutz zu blockierende Dateitypen / MIME-Typen

Alle Dateitypen und MIME-Typen (Inhaltstypen der übertragenen Daten) in der Liste werden vom Browser-Schutz blockiert.

Eingabefeld

In diesem Feld geben Sie die Namen der MIME-Typen und Dateitypen ein, die vom Browser-Schutz blockiert werden sollen. Für Dateitypen geben Sie die Datei-Extension ein, z.B. **.htm**. Für MIME-Typen notieren Sie den Medientyp und ggf. den Subtyp. Beide Angaben werden durch einen einfachen Schrägstrich voneinander getrennt, z.B. **video/mpeg** oder **audio/x-wav**.

Hinweis
Dateien, die bereits auf Ihrem Computersystem als temporäre Internetdateien gespeichert worden sind, werden zwar vom Browser-Schutz blockiert, können jedoch vom Internet-Browser lokal von Ihrem Computer geladen werden. Temporäre Internetdateien sind Dateien, die vom Internet-Browser auf Ihrem Computer gesichert werden, um Webseiten schneller anzeigen zu können.

Hinweis
Die Liste der zu blockierenden Datei- und MIME-Typen wird bei Einträgen in der Liste der auszulassenden Datei- und MIME-Typen unter Ausnahmen ignoriert.



> **Hinweis**
> Bei der Angabe von Dateitypen und MIME-Typen können Sie keine Wildcards (Platzhalter * für beliebig viele Zeichen oder ? für genau ein Zeichen) verwenden.

MIME-Typen: Beispiele für Medientypen

- `text` = für Textdateien
- `image` = für Grafikdateien
- `video` = für Videodateien
- `audio` = für Sound-Dateien
- `application` = für Dateien, die an ein bestimmtes Programm gebunden sind

Beispiele: Auszulassende Datei- und MIME-Typen

- `application/octet-stream` = Dateien des MIME-Typs application/octet-stream (ausführbare Dateien *.bin, *.exe, *.com, *dll, *.class) werden vom Browser-Schutz blockiert.
- `application/olescript` = Dateien des MIME-Typs application/olescript (ActiveX Skript-Dateien *.axs) werden vom Browser-Schutz blockiert.
- `.exe` = Alle Dateien mit der Dateierweiterung .exe (ausführbare Dateien) werden vom Browser-Schutz blockiert.
- `.msi` = Alle Dateien mit der Dateierweiterung .msi (Windows Installer Dateien) werden vom Browser-Schutz blockiert.

Hinzufügen

Mit der Schaltfläche können Sie den im Eingabefeld eingegebenen MIME- oder Dateityp in das Anzeigefenster übernehmen.

Löschen

Die Schaltfläche löscht einen markierten Eintrag in der Liste. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.

Web-Filter

Der Web-Filter verfügt über eine interne und täglich aktualisierte Datenbank, in der URLs nach Inhaltskriterien klassifiziert sind.

Web-Filter aktivieren

Bei aktivierter Option werden alle URLs, die zu den ausgewählten Kategorien in der Web-Filter-Liste zählen, blockiert.

Web-Filter-Liste

In der Web-Filter-Liste können Sie die Inhaltskategorien wählen, deren URLs vom Browser-Schutz blockiert werden sollen.

Hinweis
Der Web-Filter wird bei Einträgen in der Liste der auszulassenden URLs unter Ausnahmen ignoriert.

Hinweis
Unter **Spam URLs** werden URLs kategorisiert, die mit Spam-Emails verbreitet werden. Die Kategorie **Betrug / Täuschung** umfasst Webseiten mit 'Abonnement-Fallen' und anderen Angeboten von Dienstleistungen, deren Kosten vom Anbieter verschleiert werden.

Ausnahmen

Mit diesen Optionen können Sie MIME-Typen (Inhaltstypen der übertragenen Daten) und Dateitypen für URLs (Internetadressen) von der Suche des Browser-Schutzes ausschließen. Die angegebenen MIME-Typen und URLs werden vom Browser-Schutz ignoriert, d.h. diese Daten werden beim Übertragen auf Ihr Computersystem nicht auf Viren und Malware durchsucht.

Vom Browser-Schutz auszulassende MIME-Typen

In diesem Feld können Sie die MIME-Typen (Inhaltstypen der übertragenen Daten) auswählen, die von der Suche des Browser-Schutzes ausgenommen werden sollen.

Vom Browser-Schutz auszulassende Dateitypen / MIME-Typen (benutzerdefiniert)

Alle Dateitypen und MIME-Typen (Inhaltstypen der übertragenen Daten) in der Liste werden von der Suche des Browser-Schutzes ausgenommen.

Eingabefeld

In diesem Feld geben Sie die Namen der MIME-Typen und Dateitypen ein, die von der Suche des Browser-Schutzes ausgenommen werden sollen. Für Dateitypen geben Sie die Datei-Extension ein, z.B. `.htm`. Für MIME-Typen notieren Sie den Medientyp und ggf. den Subtyp. Beide Angaben werden durch einen einfachen Schrägstrich voneinander getrennt, z.B. `video/mpeg` oder `audio/x-wav`.

Hinweis
Bei der Angabe von Dateitypen und MIME-Typen können Sie keine Wildcards



(Platzhalter * für beliebig viele Zeichen oder ? für genau ein Zeichen) verwenden.

Warnung
Alle Dateitypen und Inhaltstypen auf der Ausschlussliste werden ohne weitere Prüfung der gesperrten Zugriffe (Liste der zu blockierenden Datei- und MIME-Typen unter Gesperrte Zugriffe) oder des Browser-Schutzes im Internet-Browser geladen: Bei allen Einträgen auf der Ausschlussliste werden die Einträge der Liste der zu blockierenden Datei- und MIME-Typen ignoriert. Es wird keine Suche nach Viren und Malware ausgeführt.

MIME-Typen: Beispiele für Medientypen

- `text` für Textdateien
- `image` = für Grafikdateien
- `video` = für Videodateien
- `audio` = für Sound-Dateien
- `application` = für Dateien, die an ein bestimmtes Programm gebunden sind

Beispiele: Auszulassende Datei-und MIME-Typen

- `audio/` = Alle Dateien vom Medientyp Audio werden von der Suche des Browser-Schutzes ausgenommen
- `video/quicktime` = Alle Videodateien vom Subtyp Quicktime (*.qt, *.mov) werden von der Suche des Browser-Schutzes ausgenommen
- `.pdf` = Alle Adobe-PDF-Dateien sind von der Suche des Browser-Schutzes ausgenommen.

Hinzufügen

Mit der Schaltfläche können Sie den im Eingabefeld eingegebenen MIME- oder Dateityp in das Anzeigefenster übernehmen.

Löschen

Die Schaltfläche löscht einen markierten Eintrag in der Liste. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.

Vom Browser-Schutz auszulassende URLs

Alle URLs in dieser Liste werden von der Suche des Browser-Schutzes ausgenommen.

Eingabefeld

In diesem Feld geben Sie URLs (Internetadressen) an, die von der Suche des Browser-Schutzes ausgenommen werden sollen, z.B. **www.domainname.com**. Sie können Teile der URL angeben, wobei Sie mit abschließenden oder führenden

Punkten den Domain-Level kennzeichnen: .domainname.de für alle Seiten und alle Subdomains der Domain. Eine Webseite mit beliebiger Top-Level-Domain (.com oder .net) notieren Sie mit einem abschließendem Punkt: **domainname.**. Wenn Sie eine Zeichenfolge ohne führenden oder abschließenden Punkt notieren, wird die Zeichenfolge als Top-Level-Domain interpretiert, z.B. **net** für alle NET-Domains (www.domain.net).

Hinweis
Bei der Angabe von URLs können Sie auch das Wildcard-Zeichen * für beliebig viele Zeichen verwenden. Verwenden Sie auch in Kombination mit Wildcards abschließende oder führende Punkte, um die Domain-Levels zu kennzeichnen:
`.domainname.*`
`*.domainname.com`
`.*name*.com` (gültig aber nicht empfohlen)
Angaben ohne Punkte wie `*name*` werden als Teile einer Top-Level-Domain interpretiert und sind nicht sinnvoll.

Warnung
Alle Webseiten auf der Liste der auszulassenden URLs werden ohne weitere Prüfung des Web-Filters oder des Browser-Schutzes im Internet-Browser geladen: Bei allen Einträgen in der Liste der auszulassenden URLs werden Einträge des Web-Filters (siehe Gesperrte Zugriffe) ignoriert. Es wird keine Suche nach Viren und Malware ausgeführt. Schließen Sie deshalb nur vertrauenswürdige URLs von der Suche des Browser-Schutzes aus.

Hinzufügen

Mit der Schaltfläche können Sie die im Eingabefeld eingegebene URL (Internetadresse) in das Anzeigefenster übernehmen.

Löschen

Die Schaltfläche löscht einen markierten Eintrag in der Liste. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.

Beispiele: Auszulassende URLs

- `www.avira.com` -ODER- `www.avira.com/*`
  = Alle URLs mit der Domain 'www.avira.com' werden von der Suche des Browser-Schutzes ausgenommen: www.avira.com/en/pages/index.php, www.avira.com/en/support/index.html, www.avira.com/en/download/index.html,..
  URLs mit der Domain www.avira.de sind nicht von der Suche des Browser-Schutzes ausgenommen.
- `avira.com` -ODER- `*.avira.com`
  = Alle URLs mit der Second- und Top-Level-Domain 'avira.com' werden von der Suche des Browser-Schutzes ausgenommen. Die Angabe impliziert alle existierenden Subdomains zu '.avira.com': www.avira.com, forum.avira.com,...

- `avira.` -ODER- `*.avira.*`
  = Alle URLs mit der Second-Level-Domain 'avira' werden von der Suche des Browser-Schutzes ausgenommen. Die Angabe impliziert alle existierenden Top-Level-Domains oder Subdomains zu '.avira.': www.avira.com, www.avira.de, forum.avira.com,...
- `.*domain*.*`
  = Alle URLs, die eine Second-Level-Domain mit der Zeichenkette 'domain' enthalten, werden von der Suche des Browser-Schutzes ausgenommen: www.domain.com, www.new-domain.de, www.sample-domain1.de, ...
- `net` -ODER- `*.net`
  = Alle URLs mit der Top-Level-Domain 'net' werden von der Suche des Browser-Schutzes ausgenommen: www.name1.net, www.name2.net,...

> **Warnung**
> Geben Sie die URLs, die Sie von der Suche des Browser-Schutzes ausschließen möchten, so präzise wie möglich an. Vermeiden Sie die Angabe gesamter Top-Level-Domains oder Teile eines Second-Level-Domainnamens, da die Gefahr besteht, dass Internetseiten, die Malware und unerwünschte Programme verbreiten durch globale Angaben unter Ausnahmen von der Suche des Browser-Schutzes ausgeschlossen werden. Es wird empfohlen mindestens die vollständige Second-Level-Domain und die Top-Level-Domain anzugeben: domainname.com

Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Suchengine.

Avira Produkte enthalten sehr leistungsfähige Heuristiken, mit denen unbekannte Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware typisch sind. Erfüllt der untersuchte Code diese charakteristischen Merkmale, wird er als verdächtig gemeldet. Dies bedeutet aber nicht zwingend, dass es sich bei dem Code tatsächlich um Malware handelt; es können auch Fehlmeldungen vorkommen. Die Entscheidung, was mit dem betreffenden Code zu geschehen hat, ist vom Nutzer selbst zu treffen, z.B. an Hand seines Wissens darüber, ob die Quelle, die den gemeldeten Code enthält, vertrauenswürdig ist.

Makrovirenheuristik

Ihr Avira Produkt enthält eine sehr leistungsfähige Makrovirenheuristik. Bei aktivierter Option werden bei möglicher Reparatur alle Makros im betroffenen Dokument gelöscht, alternativ werden verdächtige Dokumente nur gemeldet, d.h. Sie erhalten eine Warnung. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Advanced Heuristic Analysis and Detection (AHeAD)



AHeAD aktivieren

Ihr Avira Produkt beinhaltet mit der Avira AHeAD-Technologie eine sehr leistungsfähige Heuristik, die auch unbekannte (neue) Malware erkennen kann. Bei aktivierter Option können Sie hier einstellen, wie "scharf" diese Heuristik sein soll. Diese Einstellung ist standardmäßig aktiviert.

Erkennungsstufe niedrig

Bei aktivierter Option wird weniger unbekannte Malware erkannt, die Gefahr von möglichen Fehlerkennungen ist hier gering.

Erkennungsstufe mittel

Bei aktivierter Option wird ein ausgewogener Schutz mit wenigen Fehlermeldungen gewährleistet. Diese Einstellung ist standardmäßig aktiviert, wenn Sie die Anwendung dieser Heuristik gewählt haben.

Erkennungsstufe hoch

Bei aktivierter Option wird bedeutend mehr unbekannte Malware, mit Fehlmeldungen muss jedoch gerechnet werden.

12.6.2 Report

Der Browser-Schutz besitzt eine umfangreiche Protokollierfunktion, die dem Benutzer bzw. dem Administrator exakte Hinweise über die Art und Weise eines Funds geben kann.

Protokollierung

In dieser Gruppe wird der inhaltliche Umfang der Reportdatei festgelegt.

Aus

Bei aktivierter Option erstellt der Browser-Schutz kein Protokoll.
Verzichten Sie nur in Ausnahmefällen auf die Protokollierung, beispielsweise nur dann, wenn Sie Testläufe mit vielen Viren oder unerwünschten Programmen durchführen.

Standard

Bei aktivierter Option nimmt der Browser-Schutz wichtige Informationen (zu Funden, Warnungen und Fehlern) in die Reportdatei auf, weniger wichtige Informationen werden zur besseren Übersicht ignoriert. Diese Einstellung ist standardmäßig aktiviert.

Erweitert

Bei aktivierter Option nimmt der Browser-Schutz auch weniger wichtige Informationen in die Reportdatei mit auf.

Vollständig

Bei aktivierter Option nimmt der Browser-Schutz sämtliche Informationen - auch solche zu Dateigröße, Dateityp, Datum etc. - in die Reportdatei auf.

Reportdatei beschränken

Größe beschränken auf n MB

Bei aktivierter Option lässt sich die Reportdatei auf eine bestimmte Größe beschränken; mögliche Werte: 1 bis 100 MB. Bei der Beschränkung der Reportdatei wird ein Spielraum von etwa 50 Kilobytes eingeräumt, um die Belastung des Rechners niedrig zu halten. Übersteigt die Größe der Protokolldatei die angegebene Größe um 50 Kilobytes, werden automatisch so lange alte Einträge gelöscht, bis die angegebene Größe weniger 20% erreicht worden ist.

Konfiguration in Reportdatei schreiben

Bei aktivierter Option wird die verwendete Konfiguration der Echtzeitsuche in die Reportdatei geschrieben.

Hinweis
Wenn Sie keine Beschränkung der Reportdatei angegeben haben, werden automatisch ältere Einträge gelöscht, wenn die Reportdatei eine Größe von 100 MB erreicht hat. Es werden so viele Einträge gelöscht bis die Reportdatei eine Größe von 80 MB erreicht hat.

12.7 Email-Schutz

Die Rubrik Email-Schutz der Konfiguration ist für die Konfiguration des Email-Schutzes zuständig.

12.7.1 Suche

Sie nutzen den Email-Schutz, um eingehende Emails auf Viren und Malware sowie auf Spam zu prüfen. Ausgehende Emails können vom Email-Schutz auf Viren und Malware geprüft werden. Ausgehende Emails, die von einem unbekannten Bot zur Spam-Verbreitung auf ihrem Rechner gesendet werden, können vom Email-Schutz blockiert werden.

Eingehende Emails durchsuchen

Bei aktivierter Option werden eingehende Emails auf Viren und Malware sowie auf Spam geprüft. Email Schutz unterstützt die Protokolle POP3 und IMAP. Aktivieren Sie das Posteingangs-Konto, welches von Ihrem Email-Client zum Empfang von Emails genutzt wird, zur Überwachung durch den Email-Schutz.

POP3-Konten überwachen

Bei aktivierter Option werden die POP3-Konten an den angegebenen Ports überwacht.

Überwachte Ports

In diesem Feld geben Sie den Port ein, der als Posteingang vom Protokoll POP3 genutzt wird. Mehrere Ports werden durch ein Komma getrennt angegeben.

Standard

Die Schaltfläche setzt die angegebenen Ports auf den Standard-Port von POP3 zurück.

IMAP-Konten überwachen

Bei aktivierter Option werden die IMAP-Konten an den angegebenen Ports überwacht.

Überwachte Ports

In diesem Feld geben Sie den Port ein, der vom Protokoll IMAP genutzt wird. Mehrere Ports werden durch ein Komma getrennt angegeben.

Standard

Die Schaltfläche setzt die angegebenen Ports auf den Standard-Port von IMAP zurück.

Ausgehende Emails durchsuchen (SMTP)

Bei aktivierter Option werden ausgehende Emails auf Viren und Malware geprüft. Emails, die von unbekannten Bots zur Spam-Verbreitung gesendet werden, werden blockiert.

Überwachte Ports

In diesem Feld geben Sie den Port ein, der als Postausgang vom Protokoll SMTP genutzt wird. Mehrere Ports werden durch ein Komma getrennt angegeben.

Standard

Die Schaltfläche setzt die angegebenen Ports auf den Standard-Port von SMTP zurück.

> **Hinweis**
> Um die genutzten Protokolle und Ports zu verifizieren, rufen Sie in Ihrem Email-Client-Programm die Eigenschaften Ihrer Email-Konten ab. Meist werden Standard-Ports genutzt.

IPv6 Unterstützung

Bei aktivierter Option wird die Internet-Protokoll-Version 6 von Email-Schutz unterstützt. (Option nicht für Neu- oder Änderungsinstallationen unter Windows 8 verfügbar.)

Aktion bei Fund

Diese Konfigurationsrubrik enthält Einstellungen, welche Aktionen durchgeführt werden, wenn Email-Schutz einen Virus bzw. unerwünschtes Programm in einer Email oder in einem Anhang findet.

> **Hinweis**
> Die hier eingestellten Aktionen erfolgen sowohl bei einem Virenfund in eingehenden Emails als auch bei einem Virenfund in ausgehenden Emails.

Interaktiv

Bei aktivierter Option erscheint beim Fund eines Virus bzw. unerwünschten Programms in einer Email oder einem Anhang ein Dialogfenster, in dem Sie auswählen können, was mit der betroffenen Email bzw. dem Anhang geschehen soll. Diese Option ist standardmäßig aktiviert.

Fortschrittsbalken anzeigen

Bei aktivierter Option blendet der Email-Schutz während des Downloads von Emails eine Fortschrittsanzeige ein. Eine Aktivierung dieser Option ist nur möglich, wenn die Option **Interaktiv** ausgewählt wurde.

Automatisch

Bei aktivierter Option werden Sie bei Fund eines Virus bzw. unerwünschten Programms nicht mehr benachrichtigt. Der Email-Schutz reagiert nach den von Ihnen in diesem Abschnitt vorgenommenen Einstellungen.

Betroffene Emails

Die unter "*Betroffene Emails*" gewählte Option wird als primäre Aktion ausgeführt , wenn der Email-Schutz einen Virus bzw. ein unerwünschtes Programm in einer Email findet. Ist die Option "**Ignorieren"** gewählt, kann unter "*Betroffene Anhänge***"** zusätzlich ausgewählt werden, was im Falle eines Funds in einem Anhang geschehen soll.

Löschen

Bei aktivierter Option wird die betroffene Email beim Fund eines Virus bzw. unerwünschten Programms automatisch gelöscht. Der Textkörper der Email (Body) wird hierbei durch den unten angegebenen Standardtext ersetzt. Gleiches gilt für alle enthaltenen Anlagen (Attachments); diese werden ebenfalls durch einen Standardtext ersetzt.

Ignorieren

Bei aktivierter Option wird die betroffene Email trotz des Funds eines Virus bzw. unerwünschten Programms ignoriert. Sie haben jedoch noch die Möglichkeit zu entscheiden, was mit einem betroffenen Anhang geschehen soll.



In Quarantäne verschieben

Bei aktivierter Option wird die komplette Email inkl. aller Anhänge beim Fund eines Virus bzw. unerwünschten Programms in Quarantäne gestellt. Sie kann später - falls gewünscht - wieder hergestellt werden. Die betroffene Email selbst wird gelöscht. Der Textkörper der Email (Body) wird hierbei durch den unten angegebenen Standardtext ersetzt. Gleiches gilt für alle enthaltenen Anlagen (Attachments); diese werden ebenfalls durch einen Standardtext ersetzt.

Betroffene Anhänge

Die Option "**Betroffene Anhänge**" ist nur dann auswählbar, wenn unter "*Betroffene Emails*" die Einstellung "**Ignorieren**" ausgewählt wurde. Mittels dieser Option kann nun entschieden werden, was im Fall eines Funds in einem Anhang geschehen soll.

Löschen

Bei aktivierter Option wird der betroffene Anhang beim Fund eines Virus bzw. unerwünschten Programms gelöscht und durch einen Standardtext ersetzt.

Ignorieren

Bei aktivierter Option wird der Anhang trotz des Funds eines Virus bzw. unerwünschten Programms ignoriert und zugestellt.

Warnung
Wenn Sie diese Option wählen, haben Sie keinerlei Schutz vor Viren und unerwünschten Programmen durch den Email-Schutz. Wählen Sie diesen Punkt nur dann, wenn Sie genau wissen, was Sie tun. Deaktivieren Sie die Vorschau in Ihrem Email-Programm, starten Sie Anhänge auf keinen Fall per Doppelklick!

In Quarantäne verschieben

Bei aktivierter Option wird der betroffene Anhang in Quarantäne gestellt und anschließend gelöscht (durch einen Standardtext ersetzt). Der betroffene Anhang kann später - falls gewünscht - wieder hergestellt werden.

Andere Aktionen

Diese Konfigurationsrubrik enthält weitere Einstellungen, welche Aktionen durchgeführt werden, wenn der Email-Schutz einen Virus bzw. unerwünschtes Programm in einer Email oder in einer Anlage findet.

Hinweis
Die hier eingestellten Aktionen erfolgen ausschließlich bei einem Virenfund in eingehenden Emails.

Standardtext für gelöschte und verschobene Emails

Der Text in diesem Feld wird anstelle der betroffenen Email als Nachricht in die Email eingefügt. Sie können diese Nachricht editieren. Ein Text darf maximal 500 Zeichen enthalten.

Folgende Tastenkombination kann zum Formatieren verwendet werden:

Strg + Enter = Fügt einen Zeilenumbruch ein.

Standard

Die Schaltfläche fügt einen vordefinierten Standardtext in das Editierfeld ein.

Standardtext für gelöschte und verschobene Anlagen

Der Text in diesem Feld wird anstelle der betroffenen Anlage als Nachricht in die Email eingefügt. Sie können diese Nachricht editieren. Ein Text darf maximal 500 Zeichen enthalten.

Folgende Tastenkombination kann zum Formatieren verwendet werden:

Strg + Enter = Fügt einen Zeilenumbruch ein.

Standard

Die Schaltfläche fügt einen vordefinierten Standardtext in das Editierfeld ein.

Heuristik

Diese Konfigurationsrubrik enthält die Einstellungen für die Heuristik der Suchengine.

Avira Produkte enthalten sehr leistungsfähige Heuristiken, mit denen unbekannte Malware proaktiv erkannt werden kann, das heißt bevor eine spezielle Virensignatur gegen den Schädling erstellt und ein Virenschutz-Update dazu versandt wurde. Die Virenerkennung erfolgt durch eine aufwendige Analyse und Untersuchung des betreffenden Codes nach Funktionen, die für Malware typisch sind. Erfüllt der untersuchte Code diese charakteristischen Merkmale, wird er als verdächtig gemeldet. Dies bedeutet aber nicht zwingend, dass es sich bei dem Code tatsächlich um Malware handelt; es können auch Fehlmeldungen vorkommen. Die Entscheidung, was mit dem betreffenden Code zu geschehen hat, ist vom Nutzer selbst zu treffen, z.B. an Hand seines Wissens darüber, ob die Quelle, die den gemeldeten Code enthält, vertrauenswürdig ist.

Makrovirenheuristik

Ihr Avira Produkt enthält eine sehr leistungsfähige Makrovirenheuristik. Bei aktivierter Option werden bei möglicher Reparatur alle Makros im betroffenen Dokument gelöscht, alternativ werden verdächtige Dokumente nur gemeldet, d.h. Sie erhalten eine Warnung. Diese Einstellung ist standardmäßig aktiviert und wird empfohlen.

Advanced Heuristic Analysis and Detection (AHeAD)



AHeAD aktivieren

Ihr Avira Produkt beinhaltet mit der Avira AHeAD-Technologie eine sehr leistungsfähige Heuristik, die auch unbekannte (neue) Malware erkennen kann. Bei aktivierter Option können Sie hier einstellen, wie "scharf" diese Heuristik sein soll. Diese Einstellung ist standardmäßig aktiviert.

Erkennungsstufe niedrig

Bei aktivierter Option wird weniger unbekannte Malware erkannt, die Gefahr von möglichen Fehlerkennungen ist hier gering.

Erkennungsstufe mittel

Bei aktivierter Option wird ein ausgewogener Schutz mit wenigen Fehlermeldungen gewährleistet. Diese Einstellung ist standardmäßig aktiviert, wenn Sie die Anwendung dieser Heuristik gewählt haben.

Erkennungsstufe hoch

Bei aktivierter Option wird bedeutend mehr unbekannte Malware erkannt, mit Fehlmeldungen muss jedoch gerechnet werden.

AntiBot

Mit der AntiBot-Funktion des Email-Schutz verhindern Sie, dass Ihr Computer als Teil eines sogenannten Bot-Netzes zur Verbreitung von Spam-Emails missbraucht wird: Bei der Verbreitung von Spam über ein Bot-Netz infiziert in der Regel ein Angreifer zahlreiche Rechner mit einem Bot, der sich dann zu einem IRC-Server verbindet, einen bestimmten Channel betritt und dort auf den Befehl zum Versenden von Spam-Emails wartet. Um Spam-Emails eines unbekannten Bots von den Emails der Computer-Nutzer zu unterscheiden, prüft der Email-Schutz, ob der verwendete SMTP-Server und Email-Absender einer ausgehenden Email in den Listen der erlaubten Server und Absender hinterlegt sind. Ist dies nicht der Fall, wird die ausgehende Email blockiert, d.h. die Email wird nicht versandt. Die blockierte Email wird in einem Dialogfenster gemeldet.

> **Hinweis**
> Die AntiBot-Funktion kann nur genutzt werden, wenn die Suche des Email-Schutz bei ausgehenden Emails aktiv ist (siehe Option **Ausgehende Emails durchsuchen** unter Email-Schutz > Suche).

Erlaubte Server

Alle Server in dieser Liste werden vom Email-Schutz zum Email-Versand zugelassen: Emails, die an diese Server gesendet werden, werden **nicht** vom Email-Schutz blockiert. Sind in der Liste keine Server eingetragen, erfolgt bei ausgehenden Emails keine Überprüfung des verwendeten SMTP-Servers. Sind Einträge in der Liste hinterlegt, blockiert der Email-Schutz Emails, die an einen SMTP-Server gesendet werden, der nicht in der Liste hinterlegt ist.



Eingabefeld

In diesem Feld geben Sie den Hostnamen oder die IP-Adresse des SMTP-Servers ein, den Sie zum Versenden Ihrer Emails nutzen.

> **Hinweis**
> Die Angaben zu den SMTP-Servern, die von Ihrem Email-Programm zum Versenden von Emails verwendet werden, finden Sie in Ihrem Email-Programm unter den Daten der angelegten Benutzerkonten.

Hinzufügen

Mit der Schaltfläche können Sie den im Eingabefeld angegebenen Server in die Liste der erlaubten Server übernehmen.

Löschen

Die Schaltfläche löscht einen markierten Eintrag in der Liste der erlaubten Server. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.

Alle löschen

Die Schaltfläche löscht alle Einträge aus der Liste der erlaubten Server.

Erlaubte Absender

Alle Absender in dieser Liste werden vom Email-Schutz zum Email-Versand zugelassen: Emails, die von dieser Email-Adresse versendet werden, werden **nicht** vom Email-Schutz blockiert. Sind in der Liste keine Absender eingetragen, erfolgt bei ausgehenden Emails keine Überprüfung der verwendeten Absender-Email-Adresse. Sind Einträge in der Liste hinterlegt, blockiert der Email-Schutz Emails mit Absendern, die nicht in der Liste hinterlegt sind.

Eingabefeld

In diesem Feld geben Sie Ihre Email-Absender-Adresse(n) an.

Hinzufügen

Mit der Schaltfläche können Sie den im Eingabefeld angegebenen Absender in die Liste der erlaubten Absender übernehmen.

Löschen

Die Schaltfläche löscht einen markierten Eintrag in der Liste der erlaubten Absender. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist.

Alle löschen

Die Schaltfläche löscht alle Einträge in der Liste der erlaubten Absender.

12.7.2 Allgemeines

Ausnahmen

Email-Adressen, die nicht überprüft werden

Diese Tabelle zeigt Ihnen die Liste der Email-Adressen, die von der Überprüfung durch den Avira Email-Schutz ausgeschlossen wurden (Whitelist).

> **Hinweis**
> Die Liste der Ausnahmen wird ausschließlich bei eingehenden Emails vom Email-Schutz verwendet.

Email-Adressen, die nicht überprüft werden

Eingabefeld

In diesem Feld geben Sie die Email-Adresse ein, die Sie in die Liste der nicht zu prüfenden Email-Adressen hinzufügen wollen. Die Email-Adresse wird in Zukunft - abhängig von Ihren Einstellungen - nicht mehr vom Email-Schutz überprüft.

> **Hinweis**
> Bei der Eingabe von Email-Adressen können Sie Wildcards verwenden: Platzhalter ***** für beliebig viele Zeichen und Platzhalter **?** für genau ein Zeichen. Wildcards können jedoch ausschließlich bei Email-Adressen verwendet werden, die nicht auf Spam geprüft werden sollen. Daher erhalten Sie eine Fehlermeldung, wenn Sie versuchen eine Adresse mit Wildcards von der Prüfung auf Malware auszuschließen, indem Sie in der Ausschlussliste die Checkbox **Malware** aktivieren. Beachten Sie bei der Eingabe von Adressen mit Wildcards, dass die angegebene Zeichenfolge der Struktur eine Email-Adresse entsprechen muss (*@*.*).

> **Warnung**
> Beachten Sie die angegebenen Beispiele bei der Verwendung von Wildcards. Setzen Sie Wildcards nur gezielt ein und prüfen Sie genau, welche Email-Adressen Sie mit der Angabe von Wildcards in die Spam-Whitelist aufnehmen.

Beispiele: Verwendung von Wildcards in Email-Adressen (Spam-Whitelist)

- `virus@avira.*` / = Umfasst alle Emails mit dieser Adresse und beliebiger Top-Level-Domain: virus@avira.de, virus@avira.com, virus@avira.net,...
- `*@avira.com` = Umfasst alle Emails, die von der Domain **avira.com** gesendet werden: info@avira.com, virus@avira.com, kontakt@avira.com, mitarbeiter@avira.com

- `info@*.com` = Umfasst alle Email-Adressen mit der Top-Level-Domain **com** und der Adresse **info**: Die Second-Level-Domain ist beliebig: info@name1.com, info@name2.com,...

Hinzufügen

Mit der Schaltfläche können Sie die im Eingabefeld eingegebene Email-Adresse der Liste der nicht zu prüfenden Email-Adressen hinzufügen.

Löschen

Die Schaltfläche löscht eine markierte Email-Adresse in der Liste.

Email-Adresse

Email-Adresse, die nicht mehr durchsucht werden soll.

Malware

Bei aktivierter Option wird die Email-Adresse nicht mehr auf Malware überprüft.

Spam

Bei aktivierter Option wird die Email-Adresse nicht mehr auf Spam überprüft.

nach oben

Mit dieser Schaltfläche verschieben Sie eine markierte Email-Adresse um eine Position nach oben. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist oder die markierte Adresse auf der ersten Position in der Liste steht.

nach unten

Mit dieser Schaltfläche verschieben Sie eine markierte Email-Adresse um eine Position nach unten. Diese Schaltfläche ist nicht aktiv, wenn kein Eintrag markiert ist oder die markierte Adresse auf der letzten Position in der Liste steht.

Outlook Adressbuch importieren

Mit der Schaltfläche importieren Sie Email-Adressen vom Adressbuch des Email-Programms MS Outlook in die Liste der Ausnahmen. Die importierten Email-Adressen werden nicht auf Spam geprüft.

Outlook Express Adressbuch importieren (Windows XP) / Windows Mail Adressbuch importieren (Windows 7)

Mit der Schaltfläche importieren Sie Email-Adressen vom Adressbuch des Email-Programms MS Outlook Express bzw. Windows Mail in die Liste der Ausnahmen. Die importierten Email-Adressen werden nicht auf Spam geprüft.

Zwischenspeicher

Der Email-Schutz Zwischenspeicher enthält die Daten zu den durchsuchten Emails, die in der Statistik im Control Center unter **Email-Schutz** angezeigt werden.

Desweiteren werden Kopien der eingehenden Emails im Zwischenspeicher abgelegt. Die Emails werden für die Trainingsfunktionen (*Gute Email – für Training nutzen*, *Spam – für Training nutzen*) des AntiSpam Moduls genutzt.

> **Hinweis**
> Damit eingehende Emails im Zwischenspeicher gesichert werden, muss das AntiSpam Modul aktiviert sein.

Maximale Anzahl Emails im Zwischenspeicher

In diesem Feld wird die maximale Anzahl der Emails eingegeben, die der Email-Schutz im Zwischenspeicher aufbewahrt. Es werden jeweils die ältesten Emails gelöscht.

Maximale Speicherung einer Email in Tagen

In diesem Feld ist die maximale Speicherdauer einer Email in Tagen eingegeben. Nach dieser Zeit wird die Email aus dem Zwischenspeicher entfernt.

Zwischenspeicher leeren

Bei Klick auf die Schaltfläche werden die Emails, die im Zwischenspeicher aufbewahrt werden, gelöscht.

Fußzeile

Unter **Fußzeile** können Sie eine Email-Fußzeile konfigurieren, die in den Emails, die Sie senden, angezeigt wird.

Voraussetzung für die Funktion ist die Aktivierung der Email-Schutz-Prüfung für ausgehende Emails; siehe Option **Ausgehende Emails durchsuchen (SMTP)** unter **Konfiguration > Email-Schutz > Suche**. Sie können die definierte Avira Email Schutz Fußzeile nutzen, mit der Sie bestätigen, dass die gesendete Email von einem Virenschutzprogramm geprüft wurde. Sie haben auch die Möglichkeit, selbst einen Text für eine benutzerdefinierte Fußzeile einzugeben. Wenn Sie beide Optionen zur Fußzeile nutzen, wird der benutzerdefinierte Text der Avira Email-Schutz Fußzeile vorangestellt.

Fußzeile bei zu versendenden Emails

Email Schutz Fußzeile anhängen

Bei aktivierter Option wird unter dem Nachrichtentext von gesendeten Emails die Avira Email-Schutz Fußzeile angezeigt. Mit der Avira Email-Schutz Fußzeile bestätigen Sie, dass die gesendete Email vom Avira Email-Schutz auf Viren und unerwünschte



Programme geprüft wurde und nicht von einem unbekannten Bot stammt. Die Avira Email-Schutz Fußzeile enthält folgenden Text: "*Durchsucht mit Avira Email-Schutz [Produktversion] [Namenskürzel und Versionsnummer der Suchengine] [Namenskürzel und Versionsnummer der Virendefinitionsdatei]*".

Diese Fußzeile anhängen

Bei aktivierter Option wird der Text, den Sie im Eingabefeld angeben, als Fußzeile in gesendeten Emails angezeigt.

Eingabefeld

In diesem Eingabefeld können Sie einen Text eingeben, der als Fußzeile in gesendeten Emails angezeigt wird.

AntiSpam

Der Avira Email-Schutz überprüft Emails auf Viren und unerwünschte Programme. Zusätzlich verfügt er über die Fähigkeit Sie zuverlässig vor Spam-Emails zu schützen.

AntiSpam-Modul aktivieren

Bei aktivierter Option ist die AntiSpam-Funktion des Email-Schutz aktiviert.

Emailbetreff markieren

Bei aktivierter Option wird beim Erkennen einer Spam-Email dem ursprünglichen Betreff ein Hinweis hinzugefügt.

Einfach

Dem Betreff einer Spam- bzw. Phishing-Email wird ein zusätzlicher Hinweis [SPAM] bzw. [Phishing] eingefügt. Diese Option ist standardmäßig aktiviert.

Detailliert

Dem Betreff einer Spam- bzw. Phishing-Email wird ein erweiterter Hinweis über die Wahrscheinlichkeit, dass es sich um Spam handelt hinzugefügt.

Protokollieren

Bei aktivierter Option erzeugt Email-Schutz eine spezielle AntiSpam Reportdatei.

Echtzeit-Blacklisten benutzen (RBL)

Bei aktivierter Option wird in Echtzeit eine sog. "schwarze Liste" abgefragt, die zusätzliche Informationen zur Verfügung stellt, Emails zweifelhafter Herkunft als Spam zu klassifizieren.

Time-out: n Sekunde(n)

Stehen die Informationen einer Blacklist nach n Sekunden nicht zur Verfügung, wird der Versuch, die Blacklist abzurufen abgebrochen.



Trainingsdatenbank löschen

Bei Klick auf die Schaltfläche wird die Trainingsdatenbank gelöscht.

Empfänger der ausgehenden Mails automatisch der Whitelist hinzufügen

Bei aktivierter Option werden die Empfänger-Adressen von ausgehenden Emails automatisch in die Spam-Whitelist übernommen (Liste der Emails, die nicht auf Spam geprüft werden unter **Email-Schutz > Allgemeines > Ausnahmen**). Eingehende Emails, die von den Adressen der Spam-Whitelist gesendet werden, werden nicht auf Spam geprüft. Eine Prüfung auf Viren und Malware erfolgt weiterhin. Diese Option ist standardmäßig deaktiviert.

Hinweis
Diese Option kann nur aktiviert werden, wenn die Suche des Email-Schutz bei ausgehenden Emails aktiv ist (siehe Option **Ausgehende Emails durchsuchen** unter Email-Schutz > Suche).

12.7.3 Report

Der Email-Schutz besitzt eine umfangreiche Protokollierfunktion, die dem Benutzer bzw. dem Administrator exakte Hinweise über die Art und Weise eines Funds geben kann.

Protokollierung

In dieser Gruppe wird der inhaltliche Umfang der Reportdatei festgelegt.

Aus

Bei aktivierter Option erstellt der Email-Schutz kein Protokoll.
Verzichten Sie nur in Ausnahmefällen auf die Protokollierung, beispielsweise nur dann, wenn Sie Testläufe mit vielen Viren oder unerwünschten Programmen durchführen.

Standard

Bei aktivierter Option nimmt der Email-Schutz wichtige Informationen (zu Fund, Warnungen und Fehlern) in die Reportdatei auf, weniger wichtige Informationen werden zur besseren Übersicht ignoriert. Diese Einstellung ist standardmäßig aktiviert.

Erweitert

Bei aktivierter Option nimmt der Email-Schutz auch weniger wichtige Informationen in die Reportdatei mit auf.

Vollständig

Bei aktivierter Option nimmt der Email-Schutz sämtliche Informationen in die Reportdatei auf.

Reportdatei beschränken

Größe beschränken auf n MB

Bei aktivierter Option lässt sich die Reportdatei auf eine bestimmte Größe beschränken; mögliche Werte: 1 bis 100 MB. Bei der Beschränkung der Reportdatei wird ein Spielraum von etwa 50 Kilobytes eingeräumt, um die Belastung des Rechners niedrig zu halten. Übersteigt die Größe der Protokolldatei die angegebene Größe um 50 Kilobytes, werden automatisch so lange alte Einträge gelöscht, bis die angegebene Größe weniger 50 Kilobytes erreicht worden ist.

Reportdatei vor dem Kürzen sichern

Bei aktivierter Option wird die Reportdatei vor dem Kürzen gesichert.

Konfiguration in Reportdatei schreiben

Bei aktivierter Option wird die verwendete Konfiguration des Email-Schutzes in die Reportdatei geschrieben.

Hinweis
Wenn Sie keine Beschränkung der Reportdatei angegeben haben, wird automatisch eine neue Reportdatei angelegt, wenn die Reportdatei eine Größe von 100 MB erreicht hat. Es wird eine Sicherung der alten Reportdatei angelegt. Es werden bis zu drei Sicherungen alter Reportdateien vorgehalten. Die jeweils ältesten Sicherungen werden gelöscht.

12.8 Kinderschutz

Nutzen Sie Aviras *KINDERSCHUTZ* Funktionen, um ein sicheres Internet-Erlebnis für Ihre Kinder oder andere Personen, die Ihren Rechner benutzen, zu ermöglichen.

- Die Anwendung **Soziale Netzwerke** überprüft die Konten Ihrer Kinder bei sozialen Netzwerken auf Kommentare, Fotos etc., die dem Ruf des Kindes schaden könnten oder die darauf hinweisen könnten, dass sich das Kind in Gefahr befindet.
- Über die Funktion **Sicher Surfen** können Sie den Windows-Benutzern Ihres Computers Nutzerrollen zuweisen. Sie können für jede Rolle feststellen, welche URLs oder Inhaltskategorien erlaubt oder verboten werden, sowie die tägliche Nutzungsdauer des Internets oder erlaubte Nutzungszeiträume definieren.

Verwandte Themen:

- Soziale Netzwerke
- Was ist Sicher Surfen

12.8.1 Soziale Netzwerke

Dieses Kapitel enthält umfassende Informationen über

Ein Kinderschutz-Konto für Soziale Netzwerke erstellen
Mit einem bestehenden Kinderschutz-Konto für Soziale Netzwerke anmelden

Ein Konto für Soziale Netzwerke erstellen

- Vergewissern Sie sich, dass Ihr Computer mit dem Internet verbunden ist.

  Klicken Sie **Control Center > Ansicht > Kinder Schutz > Soziale Netzwerke**.

  Klicken Sie **Starten Sie jetzt**.

  ↳ Der Webbrowser öffnet die Webseite des Avira Kinderschutz für Soziale Netzwerke.

- Falls Sie einen Facebook Account besitzen, können Sie sich jetzt bei Ihrem Kinderschutz-Konto für Soziale Netzwerke anmelden, indem Sie das Facebook-Logo anklicken.

-ODER-

- Falls Sie keinen Facebook Account besitzen, geben Sie Ihren Vornamen, Ihren Nachnamen, Ihre Email-Adresse und ein Passwort in die entsprechenden Felder ein und klicken Sie **Starten Sie jetzt**.

> **Hinweis**
> Ab jetzt fungiert Ihre Email-Adresse als Ihr Benutzername.

Mit einem bestehenden Kinderschutz-Konto für Soziale Netzwerke anmelden

- Vergewissern Sie sich, dass Ihr Computer mit dem Internet verbunden ist.
- Klicken Sie **Control Center > Ansicht > Kinderschutz > Soziale Netzwerke**.

  Klicken Sie **Anmelden**.

  ↳ Wenn Sie den Cookie auf Ihrem System gespeichert haben, öffnet sich Ihr Webbrowser und zeigt sofort den Aktivitätsmonitor Ihres Avira Kinderschutz für Soziale Netzwerke an.

-ODER-

↳ Wenn Ihr Webbrowser keine Cookies speichert oder sie bei jedem Schließen des Webbrowsers löscht, können Sie sich anmelden, indem Sie entweder auf das **Facebook Logo** klicken oder Ihren Benutzernamen und Passwort eingeben.

12.8.2 Sicher Surfen

Ihr Avira Programm besitzt eine **Sicher Surfen-**Funktion zum Filtern unerwünschter oder illegaler Internetangebote und zur zeitlichen Beschränkung der Internetnutzung. Die **Sicher Surfen-**Funktion ist Teil der Komponente *KINDERSCHUTZ*.

Den Benutzern des Computers können Nutzerrollen zugewiesen werden. Eine Nutzerrolle ist konfigurierbar und umfasst ein Regelset mit folgenden Kriterien:

- Verbotene oder erlaubte URLs (Internetadressen)
- Verbotene Inhaltskategorien
- Nutzungsdauer des Internets und ggf. erlaubte Nutzungszeiträume für Wochentage

Beim Blockieren von Internetinhalten nach bestimmten Kategorien werden leistungsstarke URL-Filterlisten verwendet, in denen URLs anhand der Inhalte der Internetseiten in Inhaltsgruppen kategorisiert sind. Die URL-Filterlisten werden mehrmals stündlich aktualisiert, angepasst und erweitert. Die Rollen **Kind**, **Jugendlicher**, **Erwachsener** sind mit den entsprechenden verbotenen Kategorien vorkonfiguriert.

Die zeitliche Nutzung des Internet wird nach Internetanfragen, die in einem Mindestintervall von 5 Minuten erfolgen, erfasst.

Ist die **Sicher Surfen**-Funktion aktiv, werden beim Navigieren im Internet alle im Browser angeforderten Webseiten anhand der Nutzerrolle geprüft. Bei verbotenen Webseiten wird die Webseite blockiert und eine Meldung im Browser angezeigt. Bei einer Überschreitung der erlaubten Nutzungsdauer oder einer Nutzung außerhalb des erlaubten Zeitraums werden die angeforderten Webseiten blockiert. Es wird eine Meldung im Browser angezeigt.

Warnung
Beachten Sie, dass Sie den "**Browser-Schutz**"-Dienst aktivieren müssen, um die "**Sicher Surfen**"-Funktion nutzen zu können.

Warnung
Schützen Sie die Konfiguration Ihres Avira Produktes durch ein Kennwort, wenn Sie die **Sicher Surfen**-Funktion aktivieren. Wenn die Konfiguration nicht durch ein Kennwort geschützt ist, können alle Benutzer des Computers die Einstellungen in **Sicher Surfen** verändern oder deaktivieren. Sie aktivieren den Kennwortschutz unter Konfiguration > Allgemeines > Kennwort.

Verwandte Themen:

- Sicher Surfen aktivieren
- Eine Rolle zuweisen
- Sicher Surfen Konfiguration

Sicher Surfen aktivieren

- Öffnen Sie Avira Control Center und klicken Sie **Status** in der Navigationsleiste.



Sie müssen den **Browser-Schutz** aktivieren, um die Funktion **Sicher Surfen** nutzen zu können.

- Wenn inaktiv, aktivieren Sie den **Browser-Schutz**, indem Sie in **Status**-Ansicht unter *Internet Sicherheit* den roten Schalter neben **Browser-Schutz** klicken.

Wenn aktiv, wird der Schalter neben **Browser-Schutz** grün ("AN").

Aktivieren Sie die Funktion **Sicher Surfen**, indem Sie in **Status**-Ansicht den roten Schalter neben **Sicher Surfen** klicken.

Wenn aktiv, wird der Schalter neben Sicher Surfen grün ("AN").

- Um die Rolle eines Kindes oder einer anderer Person unter **Sicher Surfen** zu konfigurieren, klicken Sie in **Status**-Ansicht die Konfigurationsschaltfläche neben **Sicher Surfen**.

Verwandte Themen:

- Was ist Sicher Surfen
- Eine Rolle zuweisen
- Sicher Surfen Konfiguration

Eine Rolle zuweisen

Voraussetzungen:

✓ Stellen Sie sicher, dass Sie für jede Person, die Ihren Rechner nutzen darf, ein eigenes Windows-Benutzerkonto erstellt haben. Sie können in Ihrem Avira-Produkt jedem Windows-Benutzerkonto eine Sicher Surfen-Rolle zuweisen.
✓ Aktivieren Sie die Funktion **Sicher Surfen** in Ihrem Avira-Produkt.
✓ Prüfen Sie die Eigenschaften jeder Rolle, bevor Sie die Rolle einem Benutzer zuweisen.

- In **Status**-Ansicht klicken Sie die Konfigurationsschaltfläche neben **Sicher Surfen**.

- Wählen Sie den Benutzer, dem Sie eine Rolle zuweisen möchten, aus der **Benutzerauswahl**-Liste.

Die Liste enthält die Windows-Benutzerkonten, die auf Ihrem Rechner erstellt wurden.

- Klicken Sie **Hinzufügen**.

↳ Der Benutzer wird zur Liste hinzugefügt.

In Avira Internet Security sind folgende Benutzerrollen vorkonfiguriert:

- **Kind**
- **Jugendlicher**
- **Erwachsener**

Wenn Sie ein Benutzerkonto zu der Liste hinzufügen, wird die Rolle **Kind** standardmäßig zugewiesen.

- Sie können eine andere Rolle zuweisen, indem Sie die Rolle eines Benutzers mehrmals klicken.

> **Hinweis**
> Benutzer des Computers, denen keine Rolle in der Konfiguration der **Sicher Surfen**-Funktion zugewiesen wurde, werden standardmäßig vom Programm dem Benutzer **Standard** mit der Rolle **Kind** zugeordnet. Sie können auch die Rolle des **Standard**-Benutzers ändern.

- Klicken Sie **Übernehmen**, um die Konfiguration zu speichern.

Verwandte Themen:

- Eigenschaften einer Rolle ändern
- Eine Rolle hinzufügen oder löschen

Eigenschaften einer Rolle ändern

- In **Status**-Ansicht klicken Sie die Konfigurationsschaltfläche neben **Sicher Surfen**.
  - ↳ Die **Rollen**-Optionen werden im Konfigurationsfenster der Funktion **Sicher Surfen** angezeigt.
- Klicken Sie den Namen der Rolle, die Sie ändern möchten (zum Beispiel **Jugendlicher**) dann klicken Sie **Ändern**.
  - ↳ Das Fenster mit den **Eigenschaften** der Rolle erscheint.
- Führen Sie die Änderungen aus, dann klicken Sie **OK**.

Verwandte Themen:

- Eigenschaften der Rolle
- Sicher Surfen Konfiguration

Eine Rolle hinzufügen oder löschen

- In **Status**-Ansicht klicken Sie die Konfigurationsschaltfläche neben **Sicher Surfen**.
  - ↳ Die **Rollen**-Optionen werden im Konfigurationsfenster der Funktion **Sicher Surfen** angezeigt.
- Um eine Rolle zu löschen (zum Beispiel **Jugendlicher**), klicken Sie **Löschen**.

> **Hinweis**
> Sie können eine Rolle nicht löschen, solange sie einem Benutzer zugewiesen ist.

- Um eine Rolle hinzuzufügen, geben Sie einen Rollennamen (maximal 30 Zeichen) im Eingabefeld ein und klicken Sie **Hinzufügen**.

- Um die Eigenschaften der neuen Rolle anzupassen, wählen Sie die neue Rolle aus der Liste aus und klicken Sie **Ändern**.

Verwandte Themen:

- Sicher Surfen Konfiguration
- Eigenschaften der Rolle
- Eine Rolle zuweisen

Wenn Sie ein Passwort für die **Sicher Surfen**-Funktion vergeben haben, wird die **Sicher Surfen**-Konfiguration ausgeblendet und die Schaltfläche **Passwortgeschützt** angezeigt.

Passwortgeschützt

Klicken Sie die Schaltfläche "**Passwortgeschützt**" und geben Sie das Kennwort für "**Sicher Surfen**" im Fenster "**Kennwort eingeben**" ein, um die **Sicher Surfen**-Konfiguration freizuschalten.

Sicher Surfen aktivieren

Bei aktivierter Option werden alle Webseiten, die beim Navigieren im Internet angefordert werden, anhand der Rolle, die dem angemeldeten Benutzer in **Sicher Surfen** zugewiesen wurde, geprüft. Angeforderte Webseiten werden blockiert, wenn sie innerhalb der zugewiesenen Rolle als verboten eingestuft worden sind.

> **Hinweis**
> Benutzer des Computers, denen keine Rolle in der Konfiguration der **Sicher Surfen**-Funktion zugewiesen wurde, werden bei aktiviertem **Sicher Surfen** standardmäßig vom Programm dem Benutzer *Standard* mit der Rolle **Kind** zugeordnet. Sie können die Rolle des Standard-Benutzers ändern.
> Nach der Installation sind die Benutzerrollen **Kind**, **Jugendlicher** und **Erwachsener** angelegt. Bei den vorkonfigurierten Rollen ist die zeitliche Beschränkung der Internetnutzung deaktiviert.

Benutzerauswahl

Benutzer

Die Liste enthält alle Benutzer im System.

Hinzufügen

Mit der Schaltfläche können Sie den ausgewählten Benutzer zur Liste der geschützten Benutzer hinzufügen.

Löschen

Die Schaltfläche löscht einen markierten Eintrag aus der Liste.

Liste "Benutzer - Rolle"

In der Liste werden alle hinzugefügten Benutzer mit der Rolle, die dem Benutzer zugewiesen wurde, angezeigt. Beim Hinzufügen eines Benutzers wird standardmäßig vom Programm die Rolle **Kind** zugewiesen. Durch einen Mausklick auf die angezeigte Rolle haben Sie die Möglichkeit, auf eine andere Rolle zu wechseln.

> **Hinweis**
> Der *Standard*-Benutzer kann nicht gelöscht werden.

Rollen

Eingabefeld

In diesem Feld geben Sie den Namen der Rolle an, die Sie zu den Nutzerrollen hinzufügen möchten.

Ändern

Über die Schaltfläche "**Ändern**" können Sie die ausgewählte Rolle konfigurieren. Es erscheint ein Dialogfenster, in dem Sie für die Rolle verbotene und erlaubte URLs definieren sowie verbotene Webinhalte nach Kategorien auswählen können. (Siehe Eigenschaften der Rolle.)

Hinzufügen

Mit der Schaltfläche können Sie die im Eingabefeld eingegebene Rolle zur Liste der verfügbaren Rollen hinzufügen.

Löschen

Die Schaltfläche löscht eine markierte Rolle aus der Liste.

Liste

Die Liste zeigt alle eingepflegten Rollen an. Mit einem Doppelklick auf eine angezeigte Rolle können Sie den Dialog zur Definition der Rolle öffnen.

> **Hinweis**
> Die Rollen, die bereits einem Benutzer zugewiesen wurden, können nicht gelöscht werden.

Verwandte Themen:

- Was ist Sicher Surfen
- Eigenschaften der Rolle
- Nutzungsdauer
- Nutzungszeitraum



Eigenschaften der Rolle

Im Fenster **Eigenschaften der Rolle** haben Sie die Möglichkeit, eine ausgewählte Rolle zur Nutzung des Internets zu definieren.

Sie können den Zugriff auf URLs explizit erlauben oder verbieten. Sie können anhand der Auswahl bestimmter Kategorien Webinhalte blockieren. Sie haben die Möglichkeit, die Internetnutzung zeitlich zu beschränken.

Den Zugriff auf folgende URLs kontrollieren

In der Liste werden alle eingepflegten URLs mit den zugewiesenen Regeln *Blockieren* oder *Erlauben* angezeigt. Beim Hinzufügen einer URL wird standardmäßig die Regel *Blockieren* zugewiesen. Mit einem Klick auf die Regel können Sie die zugewiesene Regel wechseln.

URL hinzufügen

In diesem Feld geben Sie die URLs an, die durch die Kinderschutzfunktion kontrolliert werden sollen. Sie können Teile der URL angeben, wobei Sie mit abschließenden oder führenden Punkten den Domain-Level kennzeichnen: **.domainname.de** für alle Seiten und alle Subdomains der Domain. Eine Webseite mit beliebiger Top-Level-Domain (.com oder .net) notieren Sie mit einem abschließendem Punkt: domainname.. Wenn Sie eine Zeichenfolge ohne führenden oder abschließenden Punkt notieren, wird die Zeichenfolge als Top-Level-Domain interpretiert, z.B. **net** für alle NET-Domains (www.domain.net). Sie können auch das Wildcard-Zeichen ***** für beliebig viele Zeichen verwenden. Verwenden Sie auch in Kombination mit Wildcards abschließende oder führende Punkte, um die Domain-Levels zu kennzeichnen.

Hinweis
Die URL-Regeln werden nach der Anzahl der angegebenen Namensteile (Labels) der Domain priorisiert. Je mehr Namensteile der Domain angegeben werden desto höher ist die Priorität der Regel. Bsp.:

URL: www.avira.com - Regel: Erlauben
URL: .avira.com - Regel: Blockieren
Das Regelset erlaubt alle URLs der Domain 'www.avira.com'. Die URL 'forum.avira.com' wird blockiert.

Hinweis
Die Angaben . oder * umfassen alle URLs. Nutzen Sie diese Angaben, wenn Sie beispielsweise für die Rolle *Kind* nur wenige explizit angegebene Webseiten freigeben möchten, wie z.B. in folgendem Regelset:
URL: ***** oder **.** - Regel: Blockieren
URL: kids.yahoo.com - Regel: Erlauben
URL: kids.nationalgeographic.com - Regel: Erlauben



Das Regelset blockiert alle URLs außer den URLs mit den Domains 'kids.yahoo.com' und 'kids.nationalgeographic.com'.

Hinzufügen

Mit der Schaltfläche können Sie die eingegebene URL zur Liste der kontrollieren URLs hinzufügen.

Löschen

Die Schaltfläche löscht eine markierte URL aus der Liste der kontrollierten URLs.

Blockiere den Zugriff auf URLs die zu den folgenden Kategorien gehören

Bei aktivierter Option werden Webinhalte, die zu den ausgewählten Kategorien in der Kategorienliste zählen, blockiert.

Erlaubte Nutzungsdauer

Mit der Schaltfläche **Erlaubte Nutzungsdauer** öffnen Sie einen Dialog, in dem Sie eine zeitliche Begrenzung der Internetnutzung für die Rolle, die Sie konfigurieren, einstellen können. Sie haben die Möglichkeit, die Internetnutzung pro Monat, pro Woche oder differenziert nach Werktagen und Tagen am Wochenende festzulegen. Eine Festlegung der genauen Nutzungszeiträume pro Wochentag ist in einem weiteren Dialog möglich. Siehe Nutzungsdauer.

Beispiele: Zu kontrollierende URLs

- `www.avira.com` -ODER- `www.avira.com/*`
  = Umfasst alle URLs mit der Domain `www.avira.com`:
  www.avira.com/en/pages/index.php, *www.avira.com/en/support/index.html*, *www.avira.com/en/download/index.html*,...
  URLs mit der Domain www.avira.de sind nicht enthalten.
- `avira.com` -ODER- `*.avira.com`
  = Umfasst alle URLs mit der Second- und Top-Level-Domain `avira.com`. Die Angabe impliziert alle existierenden Subdomains zu `.avira.com`: *www.avira.com*, *forum.avira.com*,...
- `avira.` -ODER- `*.avira.*`
  = Umfasst alle URLs mit der Second-Level-Domain `avira`. Die Angabe impliziert alle existierenden Top-Level-Domains oder Subdomains zu `.avira.`:
  www.avira.com, www.avira.de, forum.avira.com,...
- `.*domain*.*`
  Umfasst alle URLs, die eine Second-Level-Domain mit der Zeichenkette '`domain`' enthalten: *www.domain.com*, *www.new-domain.de*, *www.sample-domain1.de*, ...
- `net` -ODER- `*.net`
  =Umfasst alle URLs mit der Top-Level-Domain '`net`' : *www.name1.net*, *www.name2.net*,...

Verwandte Themen:

- Was ist Sicher Surfen

- Sicher Surfen Konfiguration
- Nutzungsdauer
- Nutzungszeitraum

Nutzungsdauer

Im Fenster **Nutzungsdauer** haben Sie die Möglichkeit, eine maximale Dauer der Internetnutzung für eine Nutzerrolle festzulegen. Die zeitliche Nutzung des Internet wird nach Internetanfragen, die in einem Mindestintervall von 5 Minuten erfolgen, erfasst. Die gewünschte maximale Surfzeit für die Rolle kann pro Woche, pro Monat oder differenziert nach Werktagen und Tagen am Wochenende angegeben werden.

Internetnutzung zeitlich begrenzen

Mit der Option beschränken Sie für alle Computernutzer, die der Rolle zugewiesen sind, die Dauer der Internetnutzung. Bei einer Überschreitung der erlaubten Nutzungsdauer werden Webseiten, die der Computernutzer anfordert, d.h. aufruft, blockiert. Im Webbrowser erscheint eine Warnmeldung.

Zeitliche Begrenzungen pro Woche, Monat, pro Tag (Mo-Fr, Sa-So)

Die Angabe der gewünschten Nutzungsdauer kann über den Schieberegler oder über die Pfeiltasten rechts neben den Eingabefeldern angegeben werden. Sie können die Nutzungsdauer auch direkt in die Zeitfelder eingeben. Beachten Sie dabei das angegebene Format für die Zeitangabe.

Die verschiedenen Angaben zur Nutzungsdauer werden vom Programm nicht abgeglichen. Das Programm verwendet den jeweils geringsten zutreffenden Wert zur Beschränkung der Nutzungsdauer.

Genauer Nutzungszeitraum

Über die Schaltfläche **Genauer Nutzungszeitraum** gelangen Sie in einen Dialog, in dem Sie Tageszeiten für die definierte maximale Nutzungsdauer festlegen können. Siehe Nutzungszeitraum.

Verwandte Themen:

- Was ist Sicher Surfen
- Sicher Surfen Konfiguration
- Eigenschaften der Rolle
- Nutzungszeitraum

Nutzungszeitraum

Im Fenster **Nutzungszeitraum** legen Sie erlaubte Nutzungszeiten für die angegebene maximale Internetnutzungsdauer der Rolle fest: Sie können pro Wochentag bestimmte Tageszeiten zur Internetnutzung freigeben.

Internetnutzung nur zu den angegebenen Zeiten erlauben

Mit der Option legen Sie Tageszeiten zum "Surfen" für alle Computernutzer, die der konfigurierten Rolle zugewiesen sind, fest. Wird das Internet von den Computernutzern der Rolle außerhalb der freigegebenen Tageszeiten genutzt, werden die aufgerufenen Webseiten blockiert. Im Webbrowser erscheint eine Meldung.

- Um Tageszeiten für die Internetnutzung freizugeben, markieren Sie die gewünschten Zeitintervallen.

  Es gibt folgende Möglichkeiten, die freigegebenen bzw. gesperrten Tageszeiten zu markieren:

  - **Um Tageszeiten für die Internetnutzung freizugeben:** Klicken Sie die gewünschten unmarkierten Zeitfelder oder ziehen Sie die linke Maustaste über die unmarkierten Zeitfelder.
  - **Um Tageszeiten für die Internetnutzung zu sperren:** Klicken Sie die gewünschten markierten Zeitfelder oder ziehen Sie die linke Maustaste über die markierten Zeitfelder.

- Klicken Sie mit der rechten Maustaste in die Zeitfelder des gewünschten Tages, um die angegebenen Zeiträume in einem Dialogfenster anzuzeigen. Beispiel: *Internetnutzung gesperrt von 00:00 bis 11:00.*

Verwandte Themen:

- Was ist Sicher Surfen
- Sicher Surfen Konfiguration
- Eigenschaften der Rolle
- Nutzungsdauer

12.9 Mobiler Schutz

Avira schützt nicht nur Ihren Computer vor Malware und Viren, wir schützen auch Mobiltelefone und Smartphones, die mit dem Betriebssystem Android arbeiten, vor Diebstahl und/oder Verlust. Mithilfe der Avira Free Android Security Blockierliste können Sie desweiteren unerwünschte Anrufe und SMS fernhalten. Fügen Sie einfach Telefonnummern aus Ihrer Anruferliste, der Nachrichtenliste oder Ihren Kontakten zur Blockierliste hinzu, oder erstellen Sie manuell Kontakte, die Sie blockieren möchten.

12.9.1 Android Security

Avira Free Android Security

Avira Free Android Security besteht aus zwei Komponenten:

- Die eigentliche App, die auf dem Android-Gerät installiert wird
- Die Avira Android-Webkonsole zur Registrierung und Steuerung der Funktionen

Systemanforderungen

Betriebssystem:

- Android 2.2 (Froyo)
- Android 2.3.x (Gingerbread)
- Android 4.0.x (Ice Cream Sandwich)
- Android 4.1.x (Jelly Bean)

Arbeitsspeicher:

- 1.72 MB freier interner Arbeitsspeicher.

Browser:

- Mozilla Firefox
- Google Chrome
- Opera
- Internet Explorer IE7 oder höher.

> **Hinweis**
> Bitte beachten Sie, dass Java installiert und JavaScript aktiviert sein muss und eine funktionierende Internetverbindung erforderlich ist.

Leistungsmerkmale

Für den Fall, dass Sie Ihr Gerät nicht finden können, bietet Avira Free Android Security über die Avira Android-Webkonsole vier Funktionen zum Schutz Ihrer personenbezogenen Daten:

Signalruf-Fernauslöser

Sie lösen auf dem Gerät einen 20-sekündigen Alarm aus.

Positionsfernbestimmung

Sie aktivieren einen Positionsbefehl, der die Positionsparameter des Geräts ermittelt.

Fernsperrung

Sie können das Gerät sofort mit einer vierstelligen PIN sperren.

Fernlöschung

Sie können Daten von der SIM-Karte oder internen und externen Speicherkarten entfernen. Über die Webkonsole können Sie das Gerät zudem auf die Werkseinstellung zurücksetzen.



> **Hinweis**
> Zum Auslösen des Befehls **Zurücksetzen auf Werkseinstellung**, um bei Verlust oder Diebstahl des Geräts alle Daten zu löschen, müssen Sie während des Setups die Option **Geräteadministrator** aktivieren.

Die Funktion der Blockierliste in Avira Free Android Security ermöglicht es Ihnen, unerwünschte Anrufe und SMS fern zu halten.

Blockierliste

Sie können in die Blockierliste Kontakte aus Ihrer Anruferliste, Ihrer Nachrichtenliste oder aus Ihren Kontakten hinzufügen, oder Sie erstellen manuell einen Kontakt, den Sie blockieren möchten.

Die Webkonsole

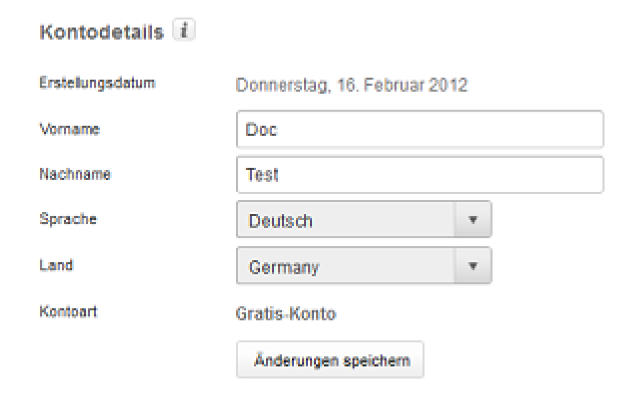
Die Avira-Webkonsole ist eine browserbasierte Anwendung zur Steuerung der Sicherheitsfunktionen. In der Startübersicht der Webkonsole können Sie Ihr Konto verwalten und Fernfunktionen, wie **Gerät suchen**, **Sperren**, **Signalruf auslösen** oder **Löschen**, auslösen.

Die Avira-Webkonsole umfasst eine Titelleiste, eine Seitenleiste und den Hauptbildschirm mit mehreren Registerkarten. In der Titelleiste werden Ihre Zugangsdaten sowie Links zum Support-Bereich und zur Kontoverwaltung angezeigt. In der Seitenleiste sind die registrierten Geräte aufgeführt. Im Hauptbildschirm der Webkonsole finden Sie alle Sicherheitsfunktionen der App, sowie Informationen zur Funktion der **Blockierliste** auf Ihrem Gerät.

Die Titelleiste der Webkonsole

Kontodetails

In der Titelleiste werden die Links zum Avira **Support**, Ihrem **Konto**, zum **Ausloggen** und Ihre Zugangsdaten angezeigt.



- Klicken Sie den Link **Konto**.



↳ Das Fenster **Kontodetails** öffnet sich mit folgenden Feldern:

Erstellungsdatum

Zeigt das Datum und die Uhrzeit an, zu der Sie das Konto registriert haben.

Vorname

Hier können Sie Ihren Vornamen eingeben.

Nachname

Hier können Sie Ihren Familiennamen eingeben.

Sprache

Wählen Sie aus dem Dropdown-Menü Ihre bevorzugte Sprache aus.

Land

Wählen Sie aus dem Dropdown-Menü ein Land aus.

Kontoart

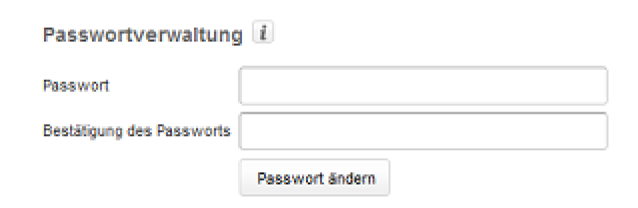
Zeigt an, welche Art von Konto Sie verwenden.

Änderungen speichern

- Klicken Sie auf **Änderungen speichern**, um die geänderten Kontodaten zu speichern.

Passwortverwaltung

Die Titelleiste der Avira Webkonsole enthält den Link zu Ihrem **Konto**, wo Sie auch Ihr Passwort verwalten.



- Klicken Sie den Link **Konto**.

  ↳ Das Fenster **Passwortverwaltung** öffnet sich mit folgenden Feldern:

Passwort

Geben Sie ein neues Passwort für Ihr Avira Free Android Security-Konto ein.

Bestätigung des Passworts

Geben Sie das Passwort zur Bestätigung erneut ein.

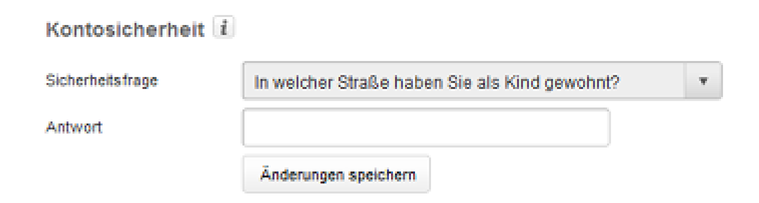


Passwort ändern

- Klicken Sie auf die Schaltfläche, um die vorgenommenen Änderungen zu speichern.

Kontosicherheit

Die Titelleiste der Avira Webkonsole enthält den Link zu Ihrem **Konto**, wo Sie auch eine Sicherheitsfrage festlegen können. Die Sicherheitsfrage dient der zusätzlichen Sicherheit Ihres Kontos. Wenn Sie Ihre Zugangsdaten vergessen oder Ihre Email-Adresse geändert haben möchten, können Sie sich mit Hilfe der Sicherheitsfrage authentifizieren.



- Klicken Sie den Link **Konto**.
  - ↳ Das Fenster **Kontosicherheit** öffnet sich mit folgenden Feldern:

Sicherheitsfrage

Öffnet das Dropdown Menü mit den Sicherheitsfragen, aus der Sie bitte eine auswählen, die nur von Ihnen persönlich beantwortet werden kann. Bitte wählen Sie eine, die individuell zu Ihnen passt.

Antwort

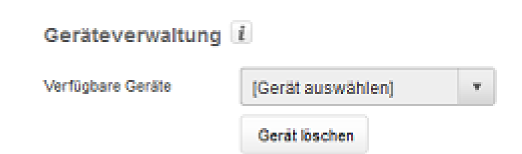
- Geben Sie Ihre Antwort in das Feld ein.
- Bitte vergewissern Sie sich, dass keine Schreibfehler in Ihrer Antwort sind und Sie sich die Antwort leicht merken können.

Änderungen speichern

- Klicken Sie Änderungen speichern, um die Sicherheitsfrage und die Antwort zu speichern.

Geräteverwaltung

Die Titelleiste der Avira Webkonsole enthält den Link zu Ihrem **Konto**, wo Sie auch Ihre Geräte verwalten.



↳ Klicken Sie den Link **Konto**.

↳ Das Fenster **Geräteverwaltung** öffnet sich mit folgenden Feldern:

Verfügbare Geräte

Öffnen Sie das Dropdown-Menü, um ein Gerät auszuwählen.

Gerät löschen

- Klicken Sie auf die Schaltfläche, um das ausgewählte Gerät aus Ihrem Konto zu löschen.

So wird es gemacht

Wie ändere ich meine Email-Adresse?

Wenden Sie sich bitte an den Avira Support, wenn Sie Ihre Email-Adresse ändern müssen. Ihre Email-Adresse dient nicht nur der Kontaktaufnahme mit Ihnen, sondern gleichzeitig auch als Ihre Benutzerkennung. Deshalb können Sie Ihre Email-Adresse nicht selbst mit der Webkonsole oder in einer App auf dem Gerät ändern.

Wie kann ich die auf meinem Gerät gespeicherten Daten schützen?

Die einfachste und schnellste Möglichkeit, Ihre auf dem Gerät gespeicherten Daten zu schützen, ist das Sperren des Geräts.

- Melden Sie sich bei der Webkonsole an.
- Navigieren Sie zur Registerkarte **Sperren**.
- Geben Sie eine vierstellige PIN ein.
- Bestätigen Sie die PIN.
- Klicken Sie auf **Sperren**.
  - ↳ Die PIN kann nunmehr zum Sperren und Entsperren des Geräts verwendet werden.

> **Hinweis**
> Die PIN ist nur vorübergehend gültig. Für jeden Befehl zum Sperren/Entsperren ist eine neue PIN erforderlich.

Wie entsperre ich mein Gerät, wenn ich die PIN vergessen beziehungsweise dreimal eine falsche PIN eingegeben habe?

> **Hinweis**
> Wenn Sie dreimal eine falsche PIN auf Ihrem Gerät eingegeben haben, müssen Sie das Gerät zunächst über die Webkonsole entsperren. Anschließend können Sie einen erneuten Sperrbefehl zu Ihrem Gerät senden.

- Melden Sie sich bei der Webkonsole an.
- Navigieren Sie zur Registerkarte **Sperren**.
- Klicken Sie die Schaltfläche **Entsperren**.
  ↳ Ihr Gerät wird sofort entsperrt.
- Geben Sie eine neue vierstellige PIN ein.
- Bestätigen Sie die PIN.
- Klicken Sie auf **Sperren**.
- Klicken Sie **OK**, um den Sperrbefehl zu bestätigen.
  ↳ Die PIN kann nunmehr zum Sperren und Entsperren des Geräts verwendet werden.

Wie ändere ich meine PIN?

Sie können Ihre PIN nur in der Webkonsole ändern. Das Ändern Ihrer PIN in der App selbst ist nicht möglich.

- Melden Sie sich bei der Webkonsole an.
- Navigieren Sie zur Registerkarte **Sperren**.
- Geben Sie eine vierstellige PIN ein.
- Bestätigen Sie die PIN.
- Klicken Sie auf **Sperren**.
  ↳ Die PIN kann nunmehr zum Sperren und Entsperren des Geräts verwendet werden.

Wie finde ich mein Gerät, wenn ich es verloren habe oder es gestohlen wurde?

Falls Sie Ihr Geräte verloren haben oder es gestohlen wurde, bietet Avira Free Android Security zwei Optionen, um es zurückzubekommen:

Auslösen eines Signalrufs

Die Funktion Signalruf auslösen erleichtert das Auffinden des Geräts. Sie ist insbesondere dann hilfreich, wenn Sie das Gerät in Ihrer unmittelbaren Umgebung, z. B. in Ihrer Wohnung, verlegt haben.

- Melden Sie sich bei der Webkonsole an.
- Wählen Sie die Registerkarte Signalruf, und klicken Sie auf Signalruf auslösen.
  ↳ Das Gerät wird jetzt 20 Sekunden lang ein lautes Geräusch abgeben, sodass es einfacher zu finden ist. Der Signalruf dauert volle 20 Sekunden und kann in diesem Zeitraum nicht abgeschaltet oder unterbrochen werden. Der Signalruf wird auch dann abgegeben, wenn das Gerät stumm geschaltet ist.



> **Hinweis**
> Bei ausgeschaltetem Gerät oder leerem Akku wird der Signalruf jedoch nicht abgegeben.

Suchen des Geräts

Wenn Sie nicht wissen, wo Sie das Gerät verloren haben oder Sie Grund zu der Annahme haben, dass es gestohlen wurde, können Sie die Position des Geräts orten.

> **Hinweis**
> Die Positionsbestimmung kann bis zu 3 Minuten dauern. Während der Ortung eines Geräts können Sie den Befehl Gerät suchen nicht erneut auslösen. Sie können den Befehl Gerät suchen aber für ein anderes, bei Ihrem Konto registriertes Gerät auslösen.

- Melden Sie sich bei der Webkonsole an.
- Wählen Sie die Registerkarte **Gerät suchen**.
  - ↳ In der Avira-Webkonsole wird ein Ausschnitt aus Google Maps angezeigt.
- Klicken Sie unterhalb der angezeigten Landkarte auf **Gerät suchen**.
- Klicken Sie **OK** um die Positionsbestimmung zu starten.
  - ↳ Die verstrichene Zeit wird während der Positionsbestimmung angezeigt. Die genaue Position des Geräts wird auf der Landkarte dargestellt. Die geophysikalischen Daten werden als Breiten- und Längengrad angezeigt.

Wie registriere ich ein neues Gerät zu einem bestehenden Konto?

Sie können Ihrem Konto bis zu 5 Geräte hinzufügen. Alle über die App zum gleichen Google-Konto oder zur gleichen Email-Adresse hinzugefügten Geräte sind für dasselbe Avira Free Android Security Konto registriert, d.h. ein Email-Konto hat ein Avira Free Android Security Konto mit bis zu 5 verschiedenen Geräten.

- Verwenden Sie das Gerät, das Sie Ihrem Konto hinzufügen möchten, zum Herunterladen von Avira Free Android Security.
- Installieren Sie die App auf dem Gerät.
- Wählen Sie entweder das Google-Konto, oder geben Sie eine andere Email-Adresse ein, und tippen Sie auf **EULA akzeptieren und fortfahren**.
  - ↳ Sie erhalten eine Email an diese Adresse, in der die Registrierung eines neuen Geräts für Ihr vorhandenes Avira Free Android Security Konto bestätigt wird.
  - ↳ Wenn Sie sich nun bei der Webkonsole anmelden, ist das neue Gerät bereits dem Bereich **Alle Ihre Geräte** auf der linken Seite der Webkonsole hinzugefügt.

- Sie können jetzt auf der Registerkarte „Gerät“ auf **Bearbeiten** klicken, um die Einstellungen zum Ändern des Gerätenamens sowie der Telefonnummer einzugeben.

> **Hinweis**
> Da einem Avira Free Android Security Konto maximal 5 Geräte hinzugefügt werden können, müssen Sie um ein weiteres Gerät zu registrieren zunächst ein bereits registriertes Gerät von Ihrem Konto und anschließend die App von diesem Gerät löschen. Navigieren Sie zuerst zu Ihren **Konto** Einstellungen in der Webkonsole Ihres Avira Free Android Security Kontos und wählen Sie ein Gerät aus der Dropdown-Liste der **Geräteverwaltung**, und klicken Sie **Gerät löschen**. Anschließend löschen Sie die App vom ausgewählten Gerät.

Problemlösung

Problemlösung

Meldung

Meldung	Bedeutung
Bitte stellen Sie eine Verbindung zu einem Mobil- oder Wi-Fi-Netz her, um fortzufahren.	Während der Registrierung wurden keine Netzverbindungen gefunden. Bitte aktivieren Sie eine Netzverbindung, um fortzufahren.
Der Dienst ist derzeit nicht verfügbar. Bitte versuchen Sie es später erneut.	Der Google-Dienst ist derzeit nicht verfügbar.
Avira Free Android Security ist abgestürzt. Bitte tippen Sie hier, um uns bei der Behebung des Fehlers zu unterstützen.	Es ist ein unerwarteter Fehler aufgetreten, daher musste die Anwendung gestoppt werden. Berühren Sie die Benachrichtigung und bestätigen Sie mit OK, um das Fehlerprotokoll automatisch an uns zu übermitteln.
Zur Registrierung des Geräts benötigen Sie ein Google-Konto. Bitte erstellen Sie ein Konto, und versuchen Sie es erneut.	Es wurde kein Google-Konto auf dem Gerät gefunden.

Das Passwort Ihres Google-Kontos wurde geändert. Öffnen Sie die Google Mail- oder Google Play-App, um das Passwort auf dem Gerät zu aktualisieren.	Das Passwort des Google-Standardkontos auf diesem Gerät ist ungültig. Bitte überprüfen Sie, ob Sie die Authentifizierung für Ihr Google-Konto geändert haben. Aktualisieren und synchronisieren Sie das Gerätepasswort durch Aufrufen der Google Mail- oder Google Play-App.
Zu viele Anwendungen auf dem Gerät verwenden den Google-Push-Dienst (GCM). Bitte deinstallieren Sie eine dieser Anwendungen, und versuchen Sie es erneut.	Google legt eine Obergrenze für auf einem Gerät installierte GCM-aktivierte Anwendungen fest.
Ein Fehler ist aufgetreten. Bitte versuchen Sie es später erneut.	Ein unbekannter Fehler ist aufgetreten.
Es sind mehr als fünf Geräte bei diesem Konto registriert. Bitte löschen Sie ein Gerät, damit ein anderes hinzugefügt werden kann.	Die Maximalanzahl von fünf bei Avira Free Android Security registrierten Geräten wurde erreicht.
Dieses Gerät ist nicht mehr für ein Avira Free Android Security Konto registriert. Daher wurde die App zurückgesetzt.	Ihre Registrierung wurde zurückgesetzt, weil dieses Gerät aus der Liste der registrierten Geräte gelöscht wurde.
Ein Server-Fehler ist aufgetreten. Bitte versuchen Sie es später erneut.	Ein unbekannter Server-Fehler ist aufgetreten.

Es ist ein unerwarteter Fehler aufgetreten, daher musste die Anwendung gestoppt werden. Helfen Sie uns bitte bei der Behebung dieses Fehlers. Klicken Sie einfach auf „OK“, und das Fehlerprotokoll wird automatisch an uns übermittelt. Sie können auch Kommentare zu diesem Fehler hinzufügen:	Die Anwendung wurde durch einen unerwarteten Fehler beendet.
Unerwarteter Fehler. Informationen finden Sie in der Benachrichtigungsleiste.	Ein unerwarteter Fehler ist aufgetreten.
Vielen Dank!	Vielen Dank für die Meldung des Problems, die Informationen wurden erfolgreich gesendet.
Bei Verlust oder Diebstahl des Geräts können Sie dieses mit Avira Free Android Security auf die Werkseinstellung zurücksetzen und somit Daten vom Gerät löschen. Um das Zurücksetzen auf Werkseinstellung vorzunehmen, muss die Funktion Geräteadministrator aktiviert sein.	Bei Verlust des Geräts können Sie mit Avira Free Android Security durch Zurücksetzen auf die Werkseinstellung Daten vom Gerät löschen. Dazu muss die Funktion **Geräteadministrator** aktiviert sein.
Löschung durch Zurücksetzen auf Werkseinstellung ist aktiviert/deaktiviert.	Die Löschfunktion mit dem Befehl **Zurücksetzen auf Werkseinstellung** ist aktiviert/deaktiviert.
Ihr Gerät wurde erfolgreich für Avira Free Android Security registriert!	Avira Free Android Security wurde erfolgreich registriert!

Eine Email wurde an <Max.Mustermann@gmail.com> gesendet. Bitte lesen Sie die Informationen und weiteren Hinweise in Ihrem Email-Konto.	Eine Email mit den Aktivierungsinformationen wurde an <Max.Mustermann@gmail.com> gesendet. Bitte lesen Sie die Email, damit Sie mit der Verwendung unserer Software beginnen können
Wenn Sie Fragen dazu haben, wenden Sie sich an das Support-Forum oder an die Mitarbeiter von Avira.	Wenn Sie Fragen dazu haben, wenden Sie sich bitte an unser Forum oder an unsere Mitarbeiter.
Registrierung fehlgeschlagen. Bitte starten Sie die App erneut, und versuchen Sie es noch einmal.	Während der Registrierung ist ein unerwarteter Fehler aufgetreten. Bitte starten Sie die Anwendung erneut, und wiederholen Sie die Registrierung.
Registrierung fehlgeschlagen. Sie verwenden möglicherweise eine Technologie, die nicht mit Avira Free Android Security kompatibel ist. Bitte starten Sie die App erneut, und versuchen Sie es noch einmal.	Ihr Gerät verwendet möglicherweise eine Technologie, die mit Avira Free Android Security nicht kompatibel ist. Bitte überprüfen Sie die folgenden Systemanforderungen: Betriebssystem: Android 2.2 (Froyo) - Android 4.1. (Jelly Bean). Arbeitsspeicher: 1,28 MB freier Arbeitsspeicher. Browser: Mozilla Firefox, Google Chrome, Opera und Internet Explorer IE7 oder höher.
Fehler beim Erstellen von Kontakt	Der Kontakt konnte nicht zur Blockierliste hinzugefügt werden, da er bereits in der Liste besteht.
Name bereits in Blockierliste vorhanden	Der Name besteht bereits in der Blockierliste und kann daher kein zweites Mal hinzugefügt werden.

Kontakt bereits in Blockierliste vorhanden	Der Kontakt besteht bereits in der Blockierliste und kann daher kein zweites Mal hinzugefügt werden.
Nummer in Blockierliste bereits vorhanden für <Max Mustermann>	Diese Telefonnummer ist bereits in der Blockierliste unter dem Eintrag <Max Mustermann> vorhanden und kann daher kein zweites Mal hinzugefügt werden.

Glossar

Abkürzung	Bedeutung
GCM	Der Android-Dienst Google-Cloud-Messaging (GCM) unterstützt das Senden von Daten von Servern zu Anwendungen auf dem Gerät.
IMEI	Die International Mobile Equipment Identity (IMEI) ist eine eindeutige Nummer, vergleichbar mit einem eindeutigen Fingerabdruck, zur Identifizierung von Geräten.
SIM-Karte	Die Teilnehmer-Identitätsmodulkarte (Subscriber Identification Module) ist eine Anbieterkarte, auf der verschiedene Informationen, wie die Seriennummer, die Telefonnummer oder die PIN, gespeichert sind.
PIN	Eine persönliche Identifikationsnummer (Personal Identification Number), meist eine vierstellige Nummer.
BS	Das Betriebssystem auf dem Gerät.
GPS	Das Global Positioning System ist ein satellitengestütztes System zur Bereitstellung von Positions- und Zeitdaten für GPS-Empfänger.



Funkzellentechnologie	Fortgeschrittene Funktechnik, mit der Signale von Mobiltelefonen empfangen und über Funkwellen an andere Funkzellen weitergegeben werden.
Wi-Fi	Ein Standard, der den Austausch von Daten und den drahtlosen Zugriff auf das Internet ermöglicht.
WLAN	Drahtloser Netzzugriff.
Cloud	Ein Remote-Serverstandort und eine IT-Infrastruktur. In der Cloud gespeicherte Daten sind nicht lokal auf Ihrem Computer gespeichert.
Alternative Telefonnummer	Die Telefonnummer, die von einem gesperrten Gerät mithilfe der Schaltfläche **Eigentümer anrufen** angerufen werden kann.
Breitengrad	Geografische Koordinate, die die Nord-Süd-Position auf der Erde angibt.
Längengrad	Geografische Koordinate, die die Ost-West-Position auf der Erde angibt.

Service

Support

Support Service

Auf unserer Webseite http://www.avira.com finden Sie alle erforderlichen Informationen zu unserem umfangreichen Support-Service.

Community Forum

Bevor Sie die Hotline kontaktieren, empfehlen wir Ihnen einen Besuch in unserem Benutzerforum unter http://forum.avira.com.
Gegebenenfalls wurde Ihr Problem innerhalb der Community schon diskutiert und gelöst.

FAQ



Bitte lesen Sie auch den Abschnitt “FAQ” auf unserer Webseite:
http://www.avira.com/de/support-for-home-knowledgebase
Möglicherweise ist Ihre Frage hier schon gestellt und von anderen Benutzern beantwortet worden.

Kontakt

Adresse

Avira Operations GmbH & Co. KG
Kaplaneiweg 1
D-88069 Tettnang
Deutschland

Internet

Weitere Informationen über uns und unsere Produkte finden Sie unter:
http://www.avira.com

Bedienung

Die Webkonsole

Nach erfolgreicher Installation müssen Sie Ihr Gerät registrieren, damit Sie die Avira-Webkonsole aufrufen können.

- Die Avira-Webkonsole umfasst eine Titelleiste, eine Seitenleiste und den Hauptbildschirm mit mehreren Registerkarten.
- In der Titelleiste werden Ihre Zugangsdaten sowie Links zum Support-Bereich und zur Kontoverwaltung angezeigt. Hier wählen Sie auch die Spracheinstellungen für die Avira Webkonsole.
- In der Seitenleiste werden die registrierten Geräte aufgeführt.
- Jedes Gerät wird auf einem separaten Feld angezeigt:
  - Klicken Sie auf der Karte des Geräts auf die Schaltfläche **Bearbeiten**, um in der Webkonsole die Registerkarte **Einstellungen** zu öffnen, auf der Sie den Namen und die Telefonnummer des Geräts verwalten können.
- Im unteren Bereich der Seitenleiste befindet sich ein Link, über den Sie eine persönliche Sicherheitsfrage angeben und speichern können.
- Im Hauptbildschirm der Webkonsole finden Sie alle Sicherheitsfunktionen um Ihr Android-Gerät zu kontrollieren, sowie Informationen zum Inhalt Ihrer Blockierliste.

Die Registerkarten der Webkonsole

Die Webkonsole hat folgende Registerkarten:

- Startübersicht
- Gerät suchen



- Löschung
- Signalruf
- Sperren
- Blockierliste
- Einstellungen

Die Startübersicht der Avira Free Android Security Webkonsole

Die Registerkarte **Startübersicht** enthält verschiedene Informationen zum jeweiligen Gerät sowie Steuerschaltflächen zum Auslösen von Aktionen, die dem Schutz des Geräts dienen.



Geräteinformation

- Marke: Die Marke des Geräts.
- Modell: Die Modellbezeichnung des Geräts.
- IMEI: Die International Mobile Equipment Identity (IMEI) ist eine eindeutige 15-stellige Nummer, mit der Mobiltelefone und auch einige Satellitentelefone identifiziert werden können.
- BS-Version: Die Versionsnummer des Android-Betriebssystems.

- App Version: Die Versionsnummer der zurzeit installierten Avira App. Wenn Sie eine veraltete Version verwenden, wird ein rotes Warnsymbol angezeigt.
- Geräteverw.: Zeigt an, ob die Geräteverwaltung aktiviert ist. Ist sie deaktiviert, wird ein rotes Warnsymbol angezeigt.
- Akku: Informationen über den Ladezustand des Akkus in Prozent.
- Telefonnummer: Die auf der SIM-Karte gespeicherte Telefonnummer.
- Netz: Das Mobilfunknetz, zu dem die SIM-Karte gehört.
- Land: Das Herkunftsland der SIM-Karte.
- **Aktualisieren**: Die Schaltfläche „Aktualisieren“ zur Aktualisierung der Geräteinformationen

Positionsbestimmung



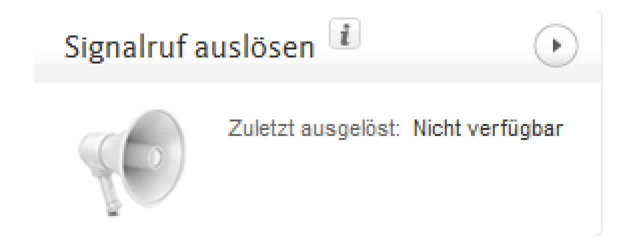
- Letzte Suche: Die Uhrzeit, zu der ein Gerät zuletzt gesucht wurde, z. B. „Vor 5 Stunden“, „Vor 3 Tagen“.
- Breitengrad: Die genaue Breitenangabe der Position des Geräts.
- Längengrad: Die genaue Längenangabe der Position des Geräts.

Gerät sperren



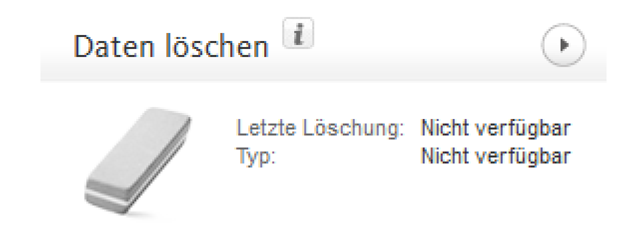
- Letzte Aktion: Die letzte Aktion, die über die Webkonsole ausgeführt wurde, z. B. „Sperren“.
- Letzte Auslösung: Die Uhrzeit, zu der ein Gerät zuletzt gesperrt bzw. entsperrt wurde.

Signalruf auslösen



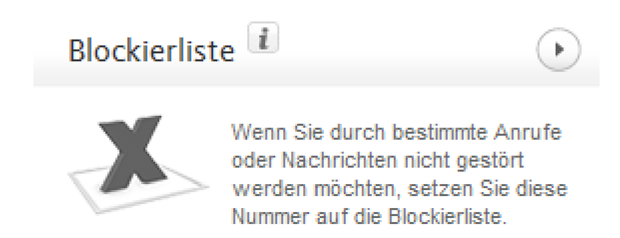
- Zuletzt ausgelöst: Der Zeitraum, seit zuletzt ein Alarm an das Gerät gesendet wurde.

Daten löschen



- Letzte Löschung: Der Zeitraum, seit zuletzt eine Löschung auf dem Gerät erfolgt ist.
- Typ: Der Typ der Löschaktion, die auf dem Gerät durchgeführt wurde.

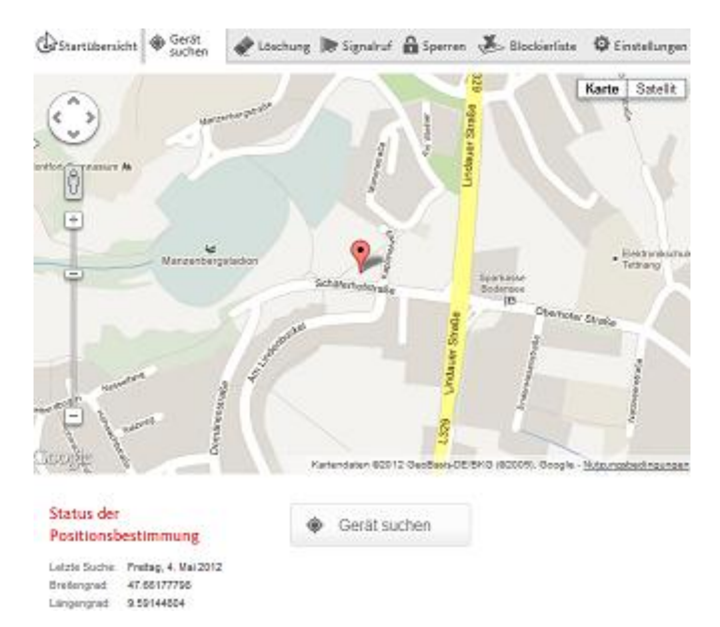
Blockierliste



- Verwenden Sie diese Funktion, um unerwünschte Anrufe und SMS fern zu halten.

Gerät suchen

Auf der Registerkarte **Gerät suchen** wird ein Ausschnitt aus Google Maps angezeigt. Der Status der Positionsbestimmung wird unterhalb der Landkarte angezeigt.



- Klicken Sie auf die Schaltfläche **Gerät suchen**, um eine Positionsbestimmung für das verlorene Gerät zu starten.
  - ↳ Die Positionsbestimmung kann je nach Netzleistung und Signalstärke mehrere Minuten dauern.

Avira Free Android Security sucht das Gerät mithilfe von GPS, der Funkzellentechnologie und von WLAN.

Die verstrichene Zeit wird während der Positionsbestimmung angezeigt.

↳ Als Ergebnis wird die genaue Position des verlorenen Geräts auf der Landkarte angezeigt. Sie können die Landkarte vergrößern und verkleinern.

Löschung

> **Hinweis**
> Wenn Ihre Version von Avira Free Android Security die Funktion **Löschung** nicht unterstützt, führen Sie ein Update der App auf dem Gerät, wie durch unsere Knowledgebase beschrieben, durch. Danach müssen Sie diese Seite nur aktualisieren, um auf die vollständige Funktionalität der **Löschfunktion** zuzugreifen.

Die Registerkarte Löschung enthält drei Optionen zum Löschen von Daten auf dem Gerät. Sie können auch eine Kombination dieser Löschoptionen auswählen. Die Löschfunktion führt zu einem dauerhaften Löschen von Daten, d. h. die von der Löschfunktion gelöschten Daten können nicht wiederhergestellt werden.

> **Hinweis**
> Es wird ausdrücklich empfohlen Ihr Gerät zu sperren, bevor Sie einen Löschbefehl durchführen. Bitte führen Sie regelmäßige ein Backup Ihrer

wichtigen Daten durch. Denn wenn die Umstände eine Fernlöschung der Daten von Ihrem Gerät erfordern, haben Sie nicht mehr die Möglichkeit ein Backup durchzuführen.

SIM-Karte

Durch Auslösen der Löschfunktion für die **SIM-Karte** werden alle Daten der SIM-Karte gelöscht. Alle auf der SIM-Karte gespeicherten Kontaktdaten und SMS werden entfernt. Diese Daten können nicht wiederhergestellt werden. Auf dem Gerät oder der SD-Karte gespeicherte Daten sind vom Löschen der SIM-Karte nicht betroffen.


SIM-Karte

Hinweis
Je nach Kartentyp ist das Löschen der **SIM-Karte** ggf. nicht möglich.

- Klicken Sie auf **SIM-Karte**, um alle auf der SIM-Karte gespeicherten Daten zu löschen.
- Bestätigen Sie das Löschen durch Klicken auf **OK**.
  - ↳ Die Meldung **Die SIM-Karte wurde erfolgreich gelöscht!** wird angezeigt.
- Klicken Sie auf **OK**, um die Meldung zu schließen und zur Registerkarte **Löschung** zurückzukehren.

Gesamter Speicher

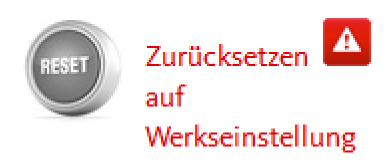
Durch Auslösen der Löschfunktion **Gesamter Speicher** werden alle auf dem Gerät oder der SD-Karte gespeicherten Daten gelöscht. Diese Daten können nicht wiederhergestellt werden. Auf der SIM-Karte gespeicherte Daten sind von der Funktion **Gesamter Speicher** nicht betroffen.



- Klicken Sie auf **Speicher löschen**, um das Löschen von direkt auf dem Gerät oder der SD-Karte gespeicherten Daten auszulösen.
- Bestätigen Sie das Löschen durch Klicken auf **OK**.
  - ↳ Die Meldung **Der Speicher wurde erfolgreich gelöscht!** wird angezeigt.
- Klicken Sie auf **OK**, um die Meldung zu schließen und zur Registerkarte **Löschung** zurückzukehren.

Zurücksetzen auf Werkseinstellung

Durch **Zurücksetzen auf Werkseinstellung** werden die Einstellungen des Geräts auf den Standardzustand zurückgesetzt und zudem alle auf dem Gerät gespeicherten Konten, Anwendungen und Anwendungsdaten gelöscht. Auf der SIM-Karte oder der SD-Karte gespeicherte Daten sind vom **Zurücksetzen auf Werkseinstellung** nicht betroffen.



> **Hinweis**
> Zum Auslösen des Befehls **Zurücksetzen auf Werkseinstellung**, um bei Verlust oder Diebstahl des Geräts alle Daten zu löschen, müssen Sie während des Setups die Funktion **Geräteadministrator** aktivieren.

- Klicken Sie auf **Zurücksetzen auf Werkseinstellung**, um die Geräteeinstellungen auf den Standardzustand zurückzusetzen.
- Bestätigen Sie diese Löschungsart durch Klicken auf **OK**.
- Klicken Sie erneut auf **OK**, um fortzufahren.
- Um die Meldung über das erfolgreiche **Zurücksetzen auf Werkseinstellung** zu schließen, klicken Sie auf **OK**.

> **Warnung**
> Durch das **Zurücksetzen auf Werkseinstellung** wird auch Avira Free Android Security deinstalliert. Sie können dann keine Befehle mehr über die Webkonsole an das Gerät senden, d. h. Sie können das Gerät nicht mehr sperren oder suchen.

Kombi-Löschung

Mit einer **Kombi-Löschung** können Sie einen, zwei oder alle drei Löschtypen gleichzeitig auslösen.

- Wählen Sie die Löschtypen aus, die Sie auslösen möchten, oder klicken Sie auf **Alles auswählen**, um eine Kombination aller Löschtypen auf einmal auszulösen.
- Klicken Sie auf **Ausgewählte Löschaktion(en) durchführen**.
- Bestätigen Sie Ihre Wahl durch Klicken auf **OK**.
  - ↳ Je nach Ihrer Auswahl und der Größe des Gerätespeichers kann diese Aktion bis zu 60 Minuten dauern.
- Klicken Sie auf **OK**, um fortzufahren.



- Um die Meldung über die erfolgreiche **Kombi-Löschung** zu schließen, klicken Sie auf **OK**.

Die Ergebnisse der drei **Löschaktionen** sehen wie folgt aus:

Betroffener Speicher	SIM-Karte	Gesamter Speicher	Zurücksetzen auf Werkseinstellung
SMS auf dem Gerät			gelöscht
SMS auf der SIM-Karte	gelöscht		
Kontaktdaten auf dem Gerät			gelöscht
Kontaktdaten auf der SIM-Karte	gelöscht		
Daten auf der SD-Karte		gelöscht	
Daten des internen USB-Speichers		gelöscht	
Konten, Anwendungen, Anwendungsdaten			gelöscht

Signalruf

Auf die Registerkarte **Signalruf** lösen Sie einen lauten Alarm aus, der von dem Gerät abgegeben wird. Mit dieser Funktion können Sie das Gerät schnell finden.





- Klicken Sie auf die Schaltfläche **Signalruf auslösen**, um die Signalruffunktion zu starten.
- Klicken Sie **OK**, um den Signalruf zu bestätigen.
  - ↳ Das Gerät gibt 20 Sekunden lang ein lautes Geräusch ab. Der Signalruf kann in diesem Zeitraum nicht abgeschaltet oder unterbrochen werden.

Sperren

Zum Sperren oder Entsperren Ihres Geräts geben Sie auf der Registerkarte **Sperren** eine vierstellige PIN ein. Sie können eine eigene Nachricht eingeben, die auf dem Sperrbildschirm des Geräts angezeigt wird. Sie können eine Telefonnummer hinzufügen, die auf dem gesperrten Gerät mithilfe der Schalfläche **Eigentümer anrufen** angerufen werden kann.



> **Hinweis**
> Es wird ausdrücklich empfohlen Ihr Gerät zu sperren, bevor Sie einen Löschbefehl durchführen. Bitte führen Sie regelmäßige ein Backup Ihrer wichtigen Daten durch. Denn wenn die Umstände eine Fernlöschung der Daten von Ihrem Gerät erfordern, haben Sie nicht mehr die Möglichkeit ein Backup durchzuführen.

- Geben Sie eine vierstellige PIN in das Feld **PIN eingeben** ein.
- Bestätigen Sie die PIN im Feld darunter.
- Klicken Sie **OK**, um das Sperren auszulösen.
  - ↳ Zum Entsperren geben Sie die vierstellige PIN auf Ihrem Gerät ein, oder klicken in Ihrem Webkonsolen Konto auf der Registerkarte **Sperren** auf die Schaltfläche **Entsperren**.
  - ↳ Sie können Ihr Gerät nur manuell entsperren,wenn Sie vorab eine PIN eingegeben haben. Wenn Sie Ihre eingegebene PIN vergessen haben, müssen Sie Ihr Gerät über die Schaltfläche **Entsperren** Ihres Webkonsolen Kontos entsperren.
- Geben Sie in das Feld **Nachricht bei verlorenem Gerät** eine Nachricht ein, die sich zur Anzeige auf dem gesperrten Gerät eignet. Geben Sie beispielsweise einen Text und Ihre Email-Adresse ein, um dem Finder den Kontakt mit Ihnen zu erleichtern.
- Geben Sie in das Feld **Alternative Telefonnummer** eine Telefonnummer ein, die auf dem gesperrten Gerät mithilfe der Schaltfläche **Eigentümer anrufen** angerufen



werden kann. Verwenden Sie eine vertrauenswürdige Telefonnummer, wie z. B. Ihre Privatnummer oder die Telefonnummer eines Freundes.

- Klicken Sie **Sperren**, um die PIN auf dem Gerät zu speichern.
- Klicken Sie **OK** um Ihr Gerät zu sperren.
- Klicken Sie auf **Entsperren**, wenn Sie das Gerät mit der Webkonsole entsperren möchten.

Blockierliste

Wenn Sie durch bestimmte Anrufe oder SMS nicht gestört werden möchten, haben Sie die Möglichkeit diese Rufnummern einfach auf die Blockierliste zu setzen. Die Funktion erlaubt Ihnen, unerwünschte Anrufe und SMS zu blockieren. Sie können Rufnummern aus Ihren Kontakten, Ihrer Anruferliste und Ihren Nachrichten hinzufügen oder manuell eine Rufnummer eingeben.



Rufnummern aus Ihren Geräte-Protokollen der Blockierliste hinzufügen

Fügen Sie Nummern aus den Protokollen Ihrer Anrufe und Nachrichten oder aus Ihren Kontakten einfach der Blockierliste hinzu.

- Öffnen Sie Avira Free Android Security auf Ihrem Gerät.
- Tippen Sie **Blockierliste**.
  ↳ Der Bildschirm **Blockierliste** öffnet sich.
- Tippen Sie die Schaltfläche **Hinzufügen**.
  ↳ Der Bildschirm **Kontakte zur Blockierliste hinzufügen** öffnet sich.
- Wählen Sie das Protokoll, aus dem Sie eine Rufnummer der Blockierliste hinzufügen möchten, und tippen Sie auf das entsprechende Feld.

  Wenn Sie keine Rufnummer auf die Blockierliste setzen möchten, tippen Sie **Abbrechen**.

  Berühren Sie die Rufnummer, die Sie blockieren möchten.

  ↳ Der Bildschirm **Kontaktdetails eingeben**zeigt Ihnen die Rufnummer und den Namen des Kontakts, den Sie blockieren möchten.
- Wählen Sie eine Blockierlistenoption. Sie haben die Möglichkeit zwischen **Anrufe & SMS**, **Anrufe** allein oder nur **SMS** auszuwählen.

- Klicken Sie **Speichern** um die Rufnummer in die Blockierliste zu speichern.
- Die blockierte Rufnummer wird auf dem Bildschirm **Blockierliste** angezeigt.

> **Hinweis**
> Wenn der Kontakt, den Sie hinzufügen möchten, bereits in der Blockierliste besteht, erhalten Sie eine Fehlermeldung.

Rufnummern manuell der Blockierliste hinzufügen

Sie können Rufnummern auch durch Eintippen in die Blockierliste einfügen.

- Öffnen Sie Avira Free Android Security auf Ihrem Gerät.
- Tippen Sie **Blockierliste**.
  - ↳ Der Bildschirm **Blockierliste** öffnet sich.
- Tippen Sie die Schaltfläche **Hinzufügen**.
  - ↳ Der Bildschirm **Kontakte zur Blockierliste hinzufügen** öffnet sich.
- Tippen Sie **Kontakt manuell erstellen**, wenn Sie eine Rufnummer eingeben möchten.
  - ↳ Der Bildschirm **Kontaktdetails eingeben** öffnet sich.
- Berühren Sie das Feld **Name** um das Tastenfeld für die Eingabe der Buchstaben zu öffnen.
- Berühren Sie das Feld **Telefonnummer** um das Tastenfeld für die Eingabe der Ziffern zu öffnen.
- Wählen Sie eine Blockierlistenoption. Sie haben die Möglichkeit zwischen **Anrufe & SMS**, **Anrufe** allein oder nur **SMS** auszuwählen.
- Klicken Sie **Speichern** um die Rufnummer in die Blockierliste zu speichern.
- Die blockierte Rufnummer wird auf dem Bildschirm **Blockierliste** angezeigt.

Editieren der Blockierliste

Sie können die Telefonnummer und den Namen Ihres blockierten Kontakts bearbeiten.

- Öffnen Sie Avira Free Android Security auf Ihrem Gerät.
- Tippen Sie **Blockierliste**.
  - ↳ Der Bildschirm **Blockierliste** öffnet sich.
- Tippen sie auf den Kontakt, den Sie bearbeiten möchten.
  - ↳ Der Bildschirm **Blockierten Kontakt editieren** öffnet sich.
- Berühren Sie das Feld **Name** um das Tastenfeld für die Bearbeitung des Namens zu öffnen.
- Berühren Sie das Feld **Telefonnummer** um das Tastenfeld für die Bearbeitung der Rufnummer zu öffnen.



- Klicken Sie **Speichern** um den bearbeiteten Kontakt in die Blockierliste zu speichern.
- Klicken Sie **Abbrechen**, wenn Sie die durchgeführten Änderungen nicht speichern möchten.

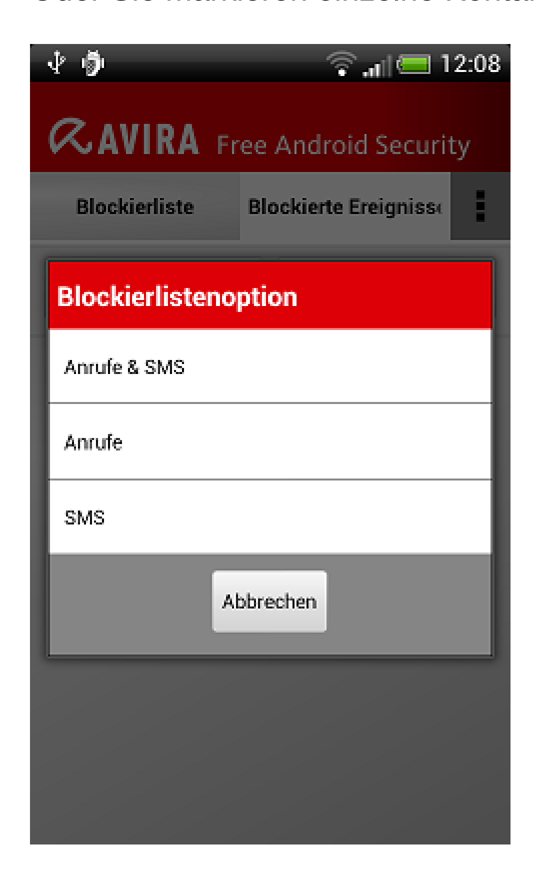
Blockierte Ereignisse

Sie können den Verlauf all Ihrer blockierten Kontakte auf der Registerkarte **Blockierte Ereignisse** überprüfen. Sie können die Liste mithilfe bestimmter Optionen filtern. Angezeigt werden der Name des Kontakts, das Datum, die Uhrzeit sowie die Art und Weise des Kontaktversuchs.

- Tippen Sie die Schaltfläche **Alle** um zwischen den Ereignissen **Alle**, **Heute** oder **Neu** auszuwählen.
- Tippen Sie die Schaltfläche **Anrufe & SMS** um sowohl blockierte Anrufe als auch Nachrichten anzeigen zu lassen. Wählen Sie die Option **Anrufe** um zu überprüfen, wer aus Ihren blockierten Kontakten versucht hat, Sie anzurufen. Oder wählen Sie **SMS**, um die Telefonnummer blockierter Textnachrichten abzurufen.

Einträge aus Blockierte Ereignisse löschen

Sie können Einträge aus **Blockierte Ereignisse** löschen. Filtern Sie die Liste blockierter Ereignisse nach **Alle**, **Heute** oder **Neu,** und wählen Sie zwischen **Anrufe & SMS**, **Anrufe** oder nur **SMS** aus. Sie können sowohl einzelne als auch alle Ereignisse löschen. Wenn Sie zum Beispiel nach **Alle** und **Anrufe** filtern, werden alle blockierten Anrufe gelistet. Sie haben dann die Möglichkeit, alle blockierten Anrufe Ihrer Kontakte zeitgleich zu löschen. Oder Sie markieren einzelne Kontakte und löschen anschließend die angezeigten Anrufe.



- Tippen Sie auf den Kontakt, dessen blockierte Ereignisse Sie löschen möchten.
  - ↳ Zeit und Anzahl der eingegangenen Anrufe und/oder SMS werden angezeigt.
- Berühren Sie das Feld **SMS**, um den Inhalt der blockierten SMS zu sehen.
  - ↳ Sie können Textnachrichten nun öffnen und lesen.
  - ↳ Sie können einzelne oder alle SMS löschen.

  Tippen Sie auf **Alle auswählen** um alle SMS für den Löschvorgang zu markieren, oder setzen Sie ein Häkchen bei einzelnen SMS.

  Tippen Sie auf **Löschen** um all diese Textnachrichten zu entfernen, oder tippen Sie auf **Zurück** um den Löschvorgang zu stoppen.

  - ↳ Sie werden aufgefordert, das Löschen der blockierten SMS zu bestätigen.

  Tippen Sie auf **Löschen** um die ausgewählten SMS aus dem Verlauf zu löschen.

  Tippen Sie auf **Abbrechen** um den Löschvorgang zu stoppen.
- Berühren Sie das Feld **Anrufe**, um alle Anrufe Ihres blockierten Kontakts zu sehen.
  - ↳ Sie können nun einzelne oder alle Anrufe löschen.

  Tippen Sie auf **Alle auswählen** um den gesamten Verlauf der Anrufe für das Löschen zu markieren, oder setzen Sie ein Häkchen bei einzelnen Anrufen.

  Tippen Sie auf **Löschen** um all diese Anrufe zu entfernen, oder tippen Sie auf **Zurück** um den Löschvorgang zu stoppen.

  - ↳ Sie werden aufgefordert, das Löschen der blockierten Anrufe zu bestätigen.

  Tippen Sie auf **Löschen** um die ausgewählten Anrufe aus dem Verlauf zu löschen.

  Tippen Sie auf **Abbrechen** um den Löschvorgang zu stoppen.

Berichte

Auf der Registerkarte **Einstellungen** werden im Bereich **Tätigkeitsbericht** alle mit der Webkonsole durchgeführten Aktivitäten von Avira Free Android Security angezeigt.

Die protokollierten Informationen sind nach Datum und Uhrzeit geordnet.

Beispiel für die vom Aktivitätsbericht angezeigten Informationen:

Datum	Uhrzeit	Meldung
Dienstag, 07. August 2012	15:17	Geräteinformationen erfolgreich aktualisiert
Dienstag, 07. August 2012	14:05	Gerät wurde gefunden

Montag, 13. August 2012	18:11	Gerät erfolgreich entsperrt

Einstellungen

Auf der Registerkarte Einstellungen verwalten Sie den Namen und die Telefonnummer des Geräts. Darüberhinaus können Sie im Bereich **Berichte** alle mit der Webkonsole durchgeführten Aktivitäten von Avira Free Android Security überprüfen.



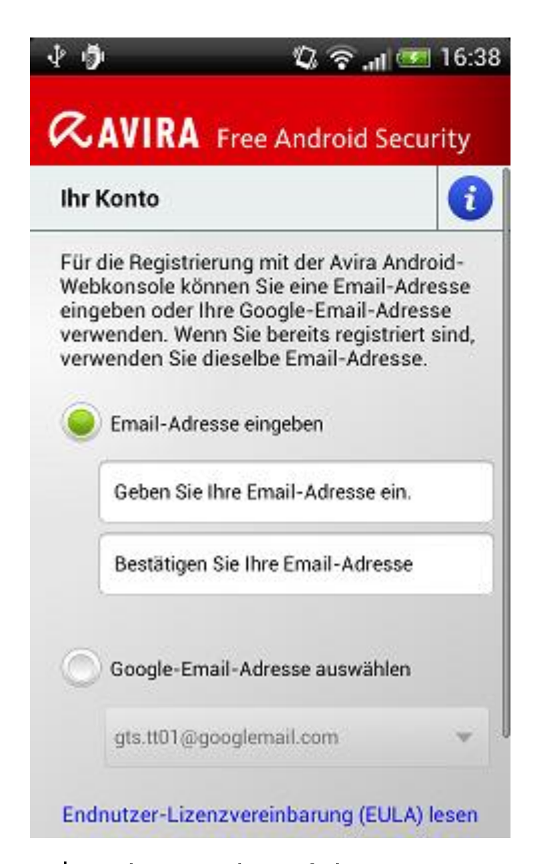
- Klicken Sie in der Navigationsleiste auf das Gerät, das Sie verwalten möchten.
- Geben Sie in das Feld **Gerätename** den Namen des Geräts ein.
- Geben Sie in das Feld **Telefonnummer** die Telefonnummer des Geräts ein.
- Klicken Sie auf **Änderungen speichern**, um die für dieses Gerät vorgenommenen Einstellungen zu speichern.
  - ↳ Die Avira Android-Webkonsole zeigt an, dass die Einstellungen erfolgreich gespeichert wurden.

Installation und Deinstallation

Installation und Deinstallation von Avira Free Android Security

Download und Installation

Laden Sie die Avira Free Android Security App direkt von Google Play auf Ihr Gerät herunter und installieren Sie die App. Nach erfolgreicher Installation werden Ihnen die neuen Funktionen vorgestellt. Danach werden Sie aufgefordert, Ihr Gerät im Registrierungsbildschirm von Avira Free Android Security zu registrieren. Dazu können Sie Ihr Google-Konto oder eine Email-Adresse eines anderen Anbieters verwenden. Für die Registrierung benötigen Sie eine stabile Internetverbindung.



- Tippen Sie auf dem Gerät **OK**, um das Registrierungsformular zu öffnen.
- Geben Sie Ihr Google-Konto oder eine andere Email-Adresse ein.
- Tippen Sie zum Fortsetzen auf **EULA akzeptieren und fortfahren**.
  - ↳ Avira sendet an die angegebene Email-Adresse eine Bestätigung für Ihr neues Avira Free Android Security Konto. Diese Bestätigungs-Email enthält einen Link, über den Sie ein persönliches Passwort für die Anmeldung bei der Android-Webkonsole festlegen können.
- Klicken Sie auf den Link in der Bestätigungs-Email, um ein Passwort einzugeben und die Android-Webkonsole zu aktivieren.
  - ↳ Die Webkonsole ermöglicht Ihnen nun die Fernkontrolle Ihrer Geräte.

Damit Avira Free Android Security zum Beispiel bei Verlust oder Diebstahl des Geräts alle Daten mit dem Befehl **Zurücksetzen auf Werkseinstellung** löschen kann, müssen Sie während des Setups die Funktion **Geräteadministrator** aktivieren:



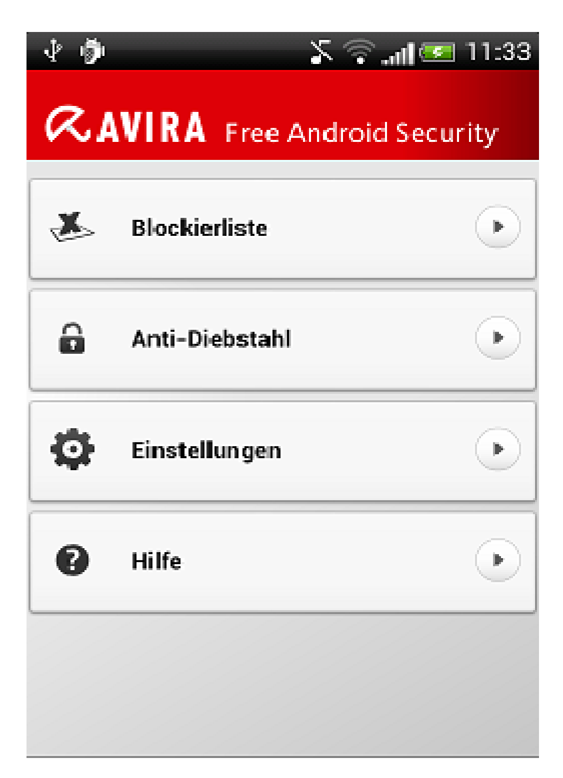


- Tippen Sie auf die Schaltfläche **Aktivieren**, um den **Geräteadministrator** zu aktivieren.
  - ↳ Der Dialog **Geräteadministrator aktivieren** wird geöffnet.
- Bestätigen Sie die Aktivierung des **Geräteadministrators**, indem Sie die Schaltfläche **Aktivieren** tippen.
  - ↳ Auf diese Weise ermöglichen Sie Avira Free Android Security alle Daten auf Ihrem Gerät zu löschen, falls Sie den Befehl **Zurücksetzen auf Werkseinstellung** durchführen wollen.

Wenn Sie sich nicht sicher sind, ob Sie die Funktion **Geräteadministrator** während des Setups installieren möchten, können Sie die Aktivierung dieser Konfigurationsoption zu jedem späteren Zeitpunkt nachholen. Bitte führen Sie die folgenden Schritte durch:

- Öffnen Sie Avira Free Android Security auf Ihrem Gerät.





- Tippen Sie auf die Fläche **Einstellungen**.
  - ↳ Nun können Sie sehen, ob die Option **Löschung durch Zurücksetzen auf Werkseinstellung** aktiviert ist.
- Tippen Sie auf die Fläche **Löscheinstellungen**.
  - ↳ Der Dialog **Geräteadministrator aktivieren** wird geöffnet. Sie werden aufgefordert die Funktion **Geräteadministrator** zu aktivieren.
- Tippen Sie auf **Aktivieren** am Ende des Dialogs.
- Bestätigen Sie die Aktivierung des **Geräteadministrators**, indem Sie die Schaltfläche **Aktivieren** tippen.
  - ↳ Sie können nun sehen, dass die Funktion **Löschung durch Zurücksetzen auf Werkseinstellung** aktiviert ist.

> **Hinweis**
> Sie können den **Geräteadministrator** jederzeit über die Avira Free Android Security App auf Ihrem Gerät aktivieren oder deaktivieren. Wählen Sie **Einstellungen > Löscheinstellungen > Löschung durch Zurücksetzen auf Werkseinstellung > Aktivieren / Deaktivieren**.

Installation über den PC

Sie können die Avira Free Android Security App über Ihren PC herunterladen.

- Öffnen Sie Google Play auf Ihrem Rechner.
- Suchen Sie nach der Avira Free Android Security App.

- Klicken Sie auf **Installieren**, um die Anwendung auf den PC herunterzuladen.
  - ↳ Sie werden aufgefordert, sich anzumelden, um die App zu installieren.
- Klicken Sie auf **Anmelden**, um Ihr Google-Konto aufzurufen.
- Geben Sie Ihre Zugangsdaten ein.
- Klicken Sie auf **OK**, um die Anwendung auf ein ausgewähltes Gerät herunterzuladen.
  - ↳ Avira Free Android Security wird auf dieses Gerät heruntergeladen.
- Klicken Sie auf **OK**, um das Download-Dialogfeld zu schließen.
  - ↳ Sie werden zurück zu Google Play geleitet, wo die Schaltfläche **Installiert** anzeigt, dass die Anwendung bereits auf das Gerät heruntergeladen wurde.

Deinstallation

Um Avira Free Android Security zu deinstallieren, müssen Sie zwei Schritte durchführen. Sie müssen die App von Ihrem Gerät und das Gerät aus Ihrem Avira Free Android Security Konto löschen.

> **Hinweis**
> Bitte vergewissern Sie sich, dass Sie die Funktion **Geräteadministrator** auf Ihrem Gerät vor einer Deinstallation von Avira Free Android Security deaktiviert haben.

Wenn Sie Avira Free Android Security deinstallieren möchten, können Sie den Deinstallationsassistenten der App selbst verwenden oder die Anwendungsverwaltung Ihres Geräts.

Wenn Sie den Deinstallationsassistenten der App verwenden, navigieren Sie von der **Hilfe** Schaltfläche zur Schaltfläche **Deinstallation durchführen**.

- Tippen Sie **Hilfe > Deinstallation durchführen > Zur Deinstallation**.
  - ↳ Die Statusinformation über Ihren Geräteadministrator öffnet sich.
- Wenn erforderlich, tippen Sie **Geräteadministrator**, um die Funktion zu deaktivieren.
- Tippen Sie **Weiter**, um mit dem Deinstallationsprozess fortzufahren.
  - ↳ Der Bildschirm Deinstallationsumfrage öffnet sich.
- Bitte wählen Sie alle Antworten aus, die auf Sie zutreffen.
- Detaillierte Anmerkungen können Sie in das Kommentarfeld schreiben.
- Tippen Sie **Weiter**, um mit der Deinstallation fortzufahren.
- Tippen Sie **OK**, um den Deinstallationsprozess abzuschließen.



Wenn Sie die App über die Anwendungsverwaltung Ihres Geräts deinstallieren möchten, navigieren Sie auf Ihrem Gerät von der Schaltfläche **Einstellungen** zur Funktion **Anwendungen verwalten**.

- Berühren Sie die Avira Free Android Security App und wählen Sie **Deinstallieren**.
- Bestätigen Sie die Deinstallation.

Außerdem müssen Sie das Gerät aus dem Avira Free Android Security Konto der Webkonsole löschen.

- Öffnen Sie die Avira-Webkonsole.
- Klicken Sie in der Titelleiste auf den Link **Konto**.
- Wechseln Sie zur Geräteverwaltung, und öffnen Sie das Dropdown-Menü **Verfügbare Geräte**.
- Wählen Sie das Gerät aus, auf dem Sie die Avira Free Android Security App löschen möchten.
- Klicken Sie auf **Gerät löschen**, um das Gerät aus Ihrem Konto zu entfernen.

Erneute Installation

Nach der Deinstallation aller Geräte können Sie nicht mehr auf die Avira-Webkonsole zugreifen.

Sie können aber unter Verwendung Ihres vorherigen Email-Kontos Avira Free Android Security erneut auf Ihrem Gerät installieren.

- Melden Sie sich mit Ihren vorherigen Zugangsdaten bei der Webkonsole an.
- Nach der Anmeldung können Sie Ihr Passwort ändern, indem Sie zur **Passwortverwaltung** navigieren.

  Wählen Sie **Konto > Passwortverwaltung**, geben Sie das neue Passwort ein und bestätigen Sie es.
- Wenn Sie Ihr Passwort vergessen haben, klicken Sie bei der Anmeldung auf den Link **Passwort vergessen?**.
  - ↳ Sie werden aufgefordert, Ihre Email-Adresse zu senden, und erhalten dann einen Wiederherstellungs-Link, damit Sie Ihr Passwort erneut festlegen können.

Erstellen des Android Kontos

Um Ihr Smartphone stets im Blick zu haben und persönliche Daten mithilfe verschiedener Fernfunktionen über die Webkonsole zu schützen, müssen Sie zunächst ein Avira Free Android Security Konto erstellen.

- Öffnen Sie das Control Center Ihres Avira Produkts.
- Klicken Sie **Control Center > Mobiler Schutz > Android Security**.
  - ↳ Die Avira Free Android Security Download-Seite wird angezeigt.



Avira Internet Security
Datei Ansicht Extras Update Hilfe

AVIRA Avira Internet Security

Status
PC SICHERHEIT
System-Scanner
Echtzeit-Scanner
Backup
INTERNET SICHERHEIT
FireWall
Browser-Schutz
Email-Schutz
KINDER SCHUTZ
Soziale Netzwerke
Sicher Surfen
MOBILER SCHUTZ
Android Security
VERWALTUNG
Quarantäne
Planer
Berichte
Ereignisse

Avira Free Android Security
Ihr Smartphone im Blick.
Auch wenn Sie es nicht sehen!
Zum Schutz des Handys vor Verlust und Diebstahl haben Sie zwei einfache Möglichkeiten:
1. Das Handy nie aus den Augen zu lassen.
2. Avira Free Android Security zu installieren.
Jetzt herunterladen
Haben Sie bereits ein Konto für Avira Free Android Security? Anmelden
Mehr Infos
Sehen Sie sich die interaktive Anleitung zu Avira Free Android Security!

- Klicken Sie **Jetzt herunterladen**.

  ↳ Die Google Play Android Apps Webseite öffnet sich.

  Klicken Sie **Installieren**.

  ↳ Sie werden aufgefordert, sich bei Google anzumelden, um die Avira Free Android Security Anwendung herunterzuladen.

  Klicken Sie **Anmelden**.

  Geben Sie Ihre Email-Adresse und Ihr Passwort ein.

  Klicken Sie **Anmelden**.

  Wählen Sie das Gerät auf das Sie Avira Free Android Security herunterladen möchten.

  Klicken Sie **Installieren**.

  ↳ Die App wird auf Ihr Android-Gerät heruntergeladen.

- Öffnen Sie Avira Free Android Security auf Ihrem Gerät.

  ↳ Die neuen Funktionen der App werden Ihnen vorgestellt. Danach werden Sie aufgefordert, Ihr Gerät im Registrierungsbildschirm von Avira Free Android Security zu registrieren. Dazu können Sie Ihr Google-Konto oder eine Email-Adresse eines anderen Anbieters verwenden.

↳ Die Bildschirmseite Ihr Konto öffnet sich.

- Geben Sie Ihre Zugangsdaten ein.
- Tippen Sie zum Fortsetzen auf **EULA akzeptieren und fortfahren**.

↳ Avira sendet Ihnen eine Bestätigungs-Email für Ihr neues Konto. Diese Bestätigungs-Email enthält einen Link, über den Sie ein persönliches Passwort für die Anmeldung bei der Android-Webkonsole festlegen können.

- Klicken Sie den Link in der Bestätigungs-Email, um ein Passwort einzugeben und die Android-Webkonsole zu aktivieren.

↳ Die Webkonsole ermöglicht Ihnen nun die Fernkontrolle Ihrer Geräte über folgende Webseite: https://android.avira.com

Sekundenschnelles Erstellen des Android Kontos

Um Ihr Smartphone stets im Blick zu haben und persönliche Daten mithilfe verschiedener Fernfunktionen über die Webkonsole zu schützen, müssen Sie zunächst ein Avira Free Android Security Konto erstellen.

- Öffnen Sie die Avira Free Android Security Webseite.

↳ Der Link zur Avira Free Android Security Download-Seite wird angezeigt.

- Klicken Sie die Schaltfläche **Jetzt anmelden!**

↳ Die Anmeldeseite öffnet sich.

- Geben Sie Ihre Google Email-Adresse oder eine andere von Ihnen bevorzugte Email-Adresse ein.

Klicken Sie **Konto erstellen**.

↳ Avira sendet an die angegebene Email-Adresse eine Bestätigungs-Email. Diese Bestätigungs-Email enthält einen Link über den Sie zur Webkonsole von Avira Free Android Security gelangen.

- Klicken Sie den Link in der Bestätigungs-Email.

↳ Sie werden zur Avira Free Android Security Webkonsole weitergeleitet.

↳ Die Webkonsole ermöglicht Ihnen nun die Fernkontrolle Ihrer Geräte mithilfe der Seite https://android.avira.com

Hinweis
Wenn Sie die eigentliche Avira Free Android Security App auf Ihr Gerät herunterladen, nachdem Sie bereits bei der Webkonsole registriert sind, achten Sie bitte darauf, dass Sie sich während des Setups mit denselben Anmeldedaten auf der Bildschirmseite **Ihr Konto** registrieren.

Anmelden an Ihrem Android Konto

- Klicken Sie **Control Center > Mobiler Schutz > Android Security**.
  - ↳ Die Avira Free Android Security Download-Seite wird angezeigt.
- Klicken Sie **Anmelden**.
  - ↳ Die Avira Free Android Security Anmeldeseite öffnet sich.
- Geben Sie Ihre registrierte Email-Adresse und Ihr Passwort ein.
- Klicken Sie **Anmelden** um die Webkonsole mit ihren Funktionen der Fernkontrolle zu öffnen.

12.10 Allgemeines

12.10.1 Gefahrenkategorien

Auswahl erweiterter Gefahrenkategorien

Ihr Avira Produkt schützt Sie vor Computerviren. Darüber hinaus haben Sie die Möglichkeit, differenziert nach folgenden Gefahrenkategorien suchen zu lassen.

- Adware
- Adware/Spyware
- Anwendungen
- Backdoor-Steuersoftware
- Dateien mit verschleierten Dateiendungen
- Kostenverursachende Einwahlprogramme
- Phishing
- Programme, die die Privatsphäre verletzen
- Scherzprogramme
- Spiele
- Trügerische Software
- Ungewöhnliche Laufzeitpacker

Durch einen Klick auf das entsprechende Kästchen wird der gewählte Typ aktiviert (Häkchen gesetzt) bzw. deaktiviert (kein Häkchen).

Alle aktivieren

Bei aktivierter Option werden sämtliche Typen aktiviert.

Standardwerte

Diese Schaltfläche stellt die vordefinierten Standardwerte wieder her.

> **Hinweis**
> Wird ein Typ deaktiviert, werden Dateien, die als entsprechender Programmtyp erkannt werden, nicht mehr gemeldet. Es erfolgt auch kein Eintrag in die Reportdatei.

12.10.2 Erweiterter Schutz

Erweiterter Schutz

ProActiv

ProActiv aktivieren

Bei aktivierter Option werden Programme auf Ihrem Computersystem überwacht und auf verdächtige Aktionen überprüft. Tritt ein Verhalten auf, das für Malware typisch ist, erhalten Sie eine Meldung. Sie können das Programm blockieren oder mit "**Ignorieren**" die Ausführung des Programms fortsetzen. Von der Überwachung ausgenommen sind: Als vertrauenswürdig eingestufte Programme, vertrauenswürdige und signierte Programme, die standardmäßig im Anwendungsfilter der erlaubten Anwendungen enthalten sind, alle Programme, die Sie zum Anwendungsfilter der erlaubten Programme hinzugefügt haben.

Mit dem Einsatz von ProActiv schützen Sie sich vor neuen und unbekannten Bedrohungen, für die noch keine Virendefinitionen und Heuristiken vorliegen. Die ProActiv-Technologie ist in die Komponente Echtzeit-Scanner integriert und beobachtet und analysiert die ausgeführten Aktionen von Programmen. Das Verhalten von Programmen wird auf typische Aktionsmuster von Malware untersucht: Art der Aktion und Aktionsabfolgen. Falls ein Programm ein für Malware typisches Verhalten zeigt, wird dies wie ein Virenfund behandelt und gemeldet: Sie haben die Möglichkeit, die Ausführung des Programms zu blockieren oder die Meldung zu ignorieren und die Ausführung des Programms fortzusetzen. Sie können das Programm als vertrauenswürdig einstufen und so zum Anwendungsfilter der erlaubten Programme hinzufügen. Sie haben auch die Möglichkeit, das Programm über die Anweisung **Immer blockieren** zum Anwendungsfilter der zu blockierenden Programme hinzuzufügen.

Zur Ermittlung des verdächtigen Verhaltens verwendet die ProActiv-Komponente Regelsets, die vom Avira Malware Research Center entwickelt wurden. Die Regelsets werden von den Avira Datenbanken gespeist. Zur Informationserfassung in den Avira Datenbanken sendet ProActiv Informationen über gemeldete, verdächtige Programme. Während der Installation von Avira, haben Sie die Möglichkeit, die Datenübermittlung an die Avira Datenbanken zu deaktivieren.

> **Hinweis**
> Die ProActiv-Technologie ist für 64-Bit-Systeme noch nicht verfügbar!

Cloud-Sicherheit

Cloud-Sicherheit aktivieren

Fingerabdrücke aller verdächtigen Dateien werden zur dynamischen Online-Erkennung an Avira Cloud übertragen. Anwendungsdateien werden sofort als sauber, infiziert oder unbekannt angezeigt.

Das Cloud-Sicherheitssystem fungiert als zentraler Knotenpunkt, um Cyber-Attacken auf die Avira-Community zu erkennen. Die Dateien, auf die Ihr PC zugreift, werden mit den Mustern der Dateien abgeglichen, die im Cloud-System gespeichert sind. Da die Hauptarbeit in der Cloud stattfindet, benötigt das lokale Schutzprogramm weniger Ressourcen.

Es wird eine Liste von Dateispeicherorten erstellt, auf welche Malware-Programme abzielen, bei jeder **Schnelle Systemprüfung**. In dieser Liste sind zum Beispiel laufende Prozesse, Start- und Dienstprogramme enthalten. Von jeder Datei wird eine digitale Prüfsumme ("Fingerabdruck") erstellt, an das Cloud-Sicherheitssystem gesendet und dann als "Clean" oder "Malware" entsprechend eingestuft. Unbekannte Programmdateien werden zur Analyse in das Cloud-Sicherheitssystem hochgeladen.

Manuell bestätigen, wenn verdächtige Dateien an Avira gesendet werden

Sie können die Liste der verdächtigen Dateien, die zur Cloud-Sicherheit hochgeladen werden sollen, prüfen und selber auswählen, welche Dateien Sie hochladen möchten.

Unter *Zu blockierende Anwendungen* können Sie Anwendungen einpflegen, die Sie als schädlich einstufen und die von Avira ProActiv standardmäßig geblockt werden sollen. Die eingepflegten Anwendungen können auf Ihrem Computersystem nicht ausgeführt werden. Sie können Programme dem Anwendungsfilter für zu blockierende Anwendungen auch über die Meldungen des Echtzeit-Scanners zu einem verdächtigen Programmverhalten hinzufügen, indem Sie die Option **Dieses Programm immer blockieren** nutzen.

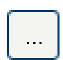
Zu blockierende Anwendungen

Anwendung

In der Liste sind alle Anwendungen aufgeführt, die Sie als schädlich eingestuft und über die Konfiguration oder über die Meldungen der ProActiv-Komponente eingefügt haben. Die Anwendungen der Liste werden von Avira ProActiv blockiert und können auf Ihrem Computersystem nicht ausgeführt werden. Beim Start eines zu blockierenden Programms erscheint eine Meldung des Betriebssystems. Die zu blockierenden Anwendungen werden von Avira ProActiv anhand des angegebenen Pfads und des Dateinamens identifiziert und unabhängig von ihrem Inhalt blockiert.

Eingabefeld

In diesem Feld geben Sie die Anwendung an, die blockiert werden soll. Zur Identifizierung der Anwendung müssen der vollständige Pfad und der Dateiname mit Dateiendung angegebenen werden. Die Pfadangabe muss entweder das Laufwerk, auf dem die Anwendung liegt, enthalten oder mit einer Umgebungsvariablen beginnen.





Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die zu blockierende Anwendung auszuwählen.

Hinzufügen

Mit der Schaltfläche "**Hinzufügen"** können Sie die im Eingabefeld angegebene Anwendung in die Liste der zu blockierenden Anwendungen übernehmen.

Hinweis
Anwendungen, die für die Funktionsfähigkeit des Betriebssystems erforderlich sind, können nicht hinzugefügt werden.

Löschen

Mit der Schaltfläche "**Löschen"** entfernen Sie eine markierte Anwendung aus der Liste der zu blockierenden Anwendungen.

Unter *Auszulassende Anwendungen* sind Anwendungen gelistet, die von der Überwachung der ProActiv-Komponente ausgenommen sind: Signierte Programme, die als vertrauenswürdig eingestuft wurden und standardmäßig in der Liste enthalten sind, alle Anwendungen, die Sie als vertrauenswürdig eingestuft und in den Anwendungsfilter eingepflegt haben: Sie können in der Konfiguration Anwendungen zur Liste der erlaubten Anwendungen hinzufügen. Sie haben auch die Möglichkeit, über die Meldungen des Echtzeit-Scanners zu einem verdächtigen Programmverhalten Anwendungen hinzuzufügen, indem Sie in der Echtzeit-Scanner-Meldung die Option **Vertrauenswürdiges Programm** nutzen.

Auszulassende Anwendungen

Anwendung

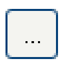
Die Liste enthält Anwendungen, die von der Überwachung der ProActiv Komponente ausgenommen sind. In den Standardeinstellungen nach der Installation enthält die Liste signierte Anwendungen von vertrauenswürdigen Herstellern. Sie haben die Möglichkeit, Anwendungen, die Sie als vertrauenswürdig einstufen, über die Konfiguration oder über Meldungen des Echtzeit-Scanners einzupflegen. Die ProActiv-Komponente identifiziert Anwendungen anhand des Pfades, des Dateinamens und des Inhalts. Eine Inhaltsprüfung ist sinnvoll, da einem Programm über Veränderungen wie Updates nachträglich Schadcode hinzugefügt werden kann. Sie können über den angegebenen **Typ** festlegen, ob eine Inhaltsprüfung erfolgen soll: Beim Typ "*Inhalt"* werden die mit Pfad und Dateinamen angegebenen Anwendungen auf Veränderungen des Dateiinhalts geprüft, bevor Sie von der Überwachung durch die ProActiv-Komponente ausgenommen werden. Bei einem veränderten Dateiinhalt wird die Anwendung von der ProActiv-Komponente wieder überwacht. Beim Typ "*Pfad"* erfolgt keine Inhaltsüberprüfung, bevor die Anwendung von der Überwachung durch den Echtzeit-Scanner ausgenommen wird. Um den Ausschlusstyp zu wechseln, klicken Sie den angezeigten Typ an.

Warnung
Verwenden Sie den Typ *Pfad* nur in Ausnahmefällen. Durch ein Update kann einer Anwendung Schadcode hinzugefügt werden. Die ursprünglich harmlose Anwendung ist nun Malware.

Hinweis
Einige vertrauenswürdige Anwendungen, wie z.B. alle Anwendungskomponenten Ihres Avira Produktes, sind standardmäßig von einer Überwachung durch die ProActiv-Komponente ausgenommen, sind aber in der Liste nicht aufgeführt.

Eingabefeld

In diesem Feld geben Sie die Anwendung an, die von der Überwachung durch die ProActiv-Komponente ausgenommen werden soll. Zur Identifizierung der Anwendung müssen der vollständige Pfad und der Dateiname mit Dateiendung angegebenen werden. Die Pfadangabe muss entweder das Laufwerk, auf dem die Anwendung liegt, enthalten oder mit einer Umgebungsvariablen beginnen.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die auszulassende Anwendung auszuwählen.

Hinzufügen

Mit der Schaltfläche "**Hinzufügen"** können Sie die im Eingabefeld angegebene Anwendung in die Liste der auszulassenden Anwendungen übernehmen.

Löschen

Mit der Schaltfläche "**Löschen"** entfernen Sie eine markierte Anwendung aus der Liste der auszulassenden Anwendungen.

12.10.3 Kennwort

Sie können Ihr Avira Produkt in unterschiedlichen Bereichen durch ein Kennwort schützen. Wurde ein Kennwort vergeben, werden Sie jedes Mal nach diesem Kennwort gefragt, wenn Sie den jeweils geschützten Bereich öffnen wollen.

Kennwort

Kennwort eingeben

Geben Sie hier Ihr gewünschtes Kennwort ein. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt. Sie können maximal 20 Zeichen eingeben. Ist das Kennwort einmal angegeben,



verweigert das Programm bei Angabe eines falschen Kennworts den Zugriff. Ein leeres Feld bedeutet "Kein Kennwort".

Bestätigung

Geben Sie hier das oben eingetragene Kennwort zur Bestätigung erneut ein. Zur Sicherheit werden die tatsächlichen Zeichen, die Sie in diesem Feld eingeben, durch Sternchen (*) ersetzt.

> **Hinweis**
> Groß- und Kleinschreibung wird unterschieden!

Kennwort geschützte Bereiche

Ihr Avira Produkt kann einzelne Bereiche durch ein Kennwort schützen. Durch Klick auf das entsprechende Kästchen kann die Kennwortabfrage für einzelne Bereiche nach Wunsch deaktiviert bzw. wieder aktiviert werden.

Kennwortgeschützer Bereich	Funktion
Control Center	Bei aktivierter Option wird zum Start des Control Center das gesetzte Kennwort benötigt.
Echtzeit-Scanner aktivieren / deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung von Avira Echtzeit-Scanner das gesetzte Kennwort benötigt.
Email-Schutz aktivieren / deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung des Email-Schutzes das gesetzte Kennwort benötigt.
FireWall aktivieren / deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung der FireWall das gesetzte Kennwort benötigt.
Browser-Schutz aktivieren/ deaktivieren	Bei aktivierter Option wird zur Aktivierung bzw. Deaktivierung des Browser-Schutzes das gesetzte Kennwort benötigt.
Sicher Surfen aktivieren / deaktivieren	Bei aktivierter Option wird zum Aktivieren bzw. Deaktivieren des Kinderschutzes das gesetzte Kennwort benötigt.



Quarantäne	Bei aktivierter Option wird zum Aktivieren bzw. Deaktivieren allen Bereichen des Quarantänemanagers das gesetzte Kennwort benötigt. Durch Klick auf das entsprechende Kästchen, kann die Kennwortabfrage nach Wunsch deaktiviert bzw. wieder aktiviert werden.
Wiederherstellen betroffener Objekte	Bei aktivierter Option wird zum Wiederherstellen eines Objekts das gesetzte Kennwort benötigt.
Erneutes Prüfen betroffener Objekte	Bei aktivierter Option wird zum erneuten Prüfen eines Objekts das gesetzte Kennwort benötigt.
Eigenschaften betroffener Objekte	Bei aktivierter Option wird zur Anzeige der Eigenschaften eines Objekts das gesetzte Kennwort benötigt.
Löschen betroffener Objekte	Bei aktivierter Option wird für das Löschen eines Objekts das gesetzte Kennwort benötigt.
Email an Avira senden	Bei aktivierter Option wird für das Versenden eines Objekts zur Überprüfung an das Avira Malware Research Center das gesetzte Kennwort benötigt.
Kopieren betroffener Objekte	Bei aktivierter Option wird für das Kopieren von betroffenen Objekten das gesetzte Kennwort benötigt.
Hinzufügen und Ändern von Aufträgen	Bei aktivierter Option wird beim Hinzufügen und Ändern von Aufträgen im Planer das gesetzte Kennwort benötigt.
Konfiguration	Bei aktivierter Option ist die Konfiguration des Programms nur nach Eingabe des gesetzten Kennworts möglich.
Installation / Deinstallation	Bei aktivierter Option wird zur Installation bzw. Deinstallation des Programms das gesetzte Kennwort benötigt.

12.10.4 Sicherheit

Autorun

Autorun-Funktion blockieren

Bei aktivierter Option wird die Ausführung der Windows Autorun-Funktion auf allen eingebundenen Laufwerken wie USB-Sticks, CD- und DVD-Laufwerken, Netzlaufwerken blockiert. Mit der Windows Autorun-Funktion werden Dateien auf Datenträgern oder Netzlaufwerken beim Einlegen oder beim Verbinden sofort gelesen, Dateien können so automatisch gestartet und wiedergegeben werden. Diese Funktionalität birgt jedoch ein hohes Sicherheitsrisiko, da mit dem automatischen Start von Dateien Malware und unerwünschte Programme installiert werden können. Besonders kritisch ist die Autorun-Funktion für USB-Sticks, da sich Daten auf einem Stick ständig ändern können.

CDs und DVDs ausnehmen

Bei aktivierter Option wird die Autorun-Funktion auf CD- und DVD-Laufwerken zugelassen.

Warnung
Deaktivieren Sie die Autorun-Funktion für CD- und DVD-Laufwerke nur dann, wenn Sie sicher sind, dass Sie ausschließlich vertrauenswürdige Datenträger verwenden.

Systemschutz

Windows hosts Datei vor Änderungen schützen

Ist diese Option aktiviert, ist die Windows hosts Datei schreibgeschützt. Eine Manipulation der Datei ist dann nicht länger möglich. Malware ist dann beispielsweise nicht mehr in der Lage, Sie auf unerwünschte Webseiten umzuleiten. Diese Option ist standardmäßig aktiviert.

Produktschutz

Hinweis
Die Optionen zum Produktschutz sind nicht verfügbar, wenn der Echtzeit-Scanner bei einer benutzerdefinierten Installation nicht installiert wurde.

Prozesse vor unerwünschtem Beenden schützen

Bei aktivierter Option werden alle Prozesse des Programms vor unerwünschtem Beenden durch Viren und Malware oder vor einem 'unkontrollierten' Beenden durch einen Benutzer z.B. via Task-Manager geschützt. Diese Option ist standardmäßig aktiviert.

Erweiterter Prozessschutz

Bei aktivierter Option werden alle Prozesse des Programms vor unerwünschtem Beenden mit erweiterten Methoden geschützt. Der erweiterte Prozessschutz benötigt erheblich mehr Rechnerressourcen als der einfache Prozessschutz. Die Option ist standardmäßig aktiviert. Zum Deaktivieren der Option ist ein Rechnerneustart erforderlich.

Hinweis
Der Prozessschutz ist unter Windows XP 64 Bit nicht verfügbar!

Warnung
Bei aktiviertem Prozessschutz können Interaktionsprobleme mit anderen Softwareprodukten auftreten. Deaktivieren Sie in diesen Fällen den Prozessschutz.

Dateien und Registrierungseinträge vor Manipulation schützen

Bei aktivierter Option werden alle Registry-Einträge des Programms sowie alle Dateien des Programms (Binär- und Konfigurationsdateien) vor Manipulation geschützt. Der Schutz vor Manipulation beinhaltet den Schutz vor schreibendem, löschendem und z.T. lesendem Zugriff auf die Registry-Einträge oder die Programmdateien durch Benutzer oder fremde Programme. Zum Aktivieren der Option ist ein Rechnerneustart erforderlich.

Warnung
Beachten Sie, dass bei deaktivierter Option die Reparatur von Computern, die mit bestimmten Arten von Malware infiziert sind, fehlschlagen kann.

Hinweis
Bei aktivierter Option sind Änderungen an der Konfiguration, so auch die Änderung von Prüf- oder Update-Aufträgen nur über die Benutzeroberfläche möglich.

Hinweis
Der Schutz von Dateien und Registrierungseinträgen ist unter Windows XP 64 Bit nicht verfügbar!

12.10.5 WMI

Unterstützung für Windows Management Instrumentation (WMI)



Windows Management Instrumentation ist eine grundlegende Windows Verwaltungstechnologie, die es ermöglicht mittels Skript- und Programmiersprachen lesend und schreibend, lokal und remote auf Einstellungen von Windows Rechnern zuzugreifen. Ihr Avira Produkt unterstützt WMI und stellt Daten (Statusinformationen, Statistik-Daten, Reports, geplante Aufträge etc.) sowie Ereignisse an einer Schnittstelle zur Verfügung. Sie haben über WMI die Möglichkeit, Betriebsdaten des Programms abzurufen.

WMI-Unterstützung aktivieren

Bei aktivierter Option haben Sie die Möglichkeit, über WMI Betriebsdaten des Programms abzurufen.

12.10.6 Ereignisse

Größe der Ereignisdatenbank begrenzen

Größe begrenzen auf maximal n Einträge

Bei aktivierter Option kann die maximale Anzahl der Einträge in der Ereignisdatenbank auf eine bestimmte Größe begrenzt werden; erlaubte Werte sind: 100 bis 10 000 Einträge. Wird die Anzahl der eingegebenen Einträge überschritten, werden die jeweils ältesten Einträge gelöscht.

Alle Ereignisse löschen älter als n Tag(e)

Bei aktivierter Option werden Ereignisse nach einer gewissen Anzahl von Tagen aus der Ereignisdatenbank gelöscht; erlaubte Werte sind: 1 bis 90 Tage. Diese Option ist standardmäßig mit einem Wert von 30 Tagen aktiviert.

Keine Begrenzung

Bei aktivierter Option ist die Größe der Ereignisdatenbank nicht begrenzt. Auf der Programmoberfläche unter Ereignisse werden jedoch maximal 20 000 Einträge angezeigt.

12.10.7 Berichte

Berichte begrenzen

Anzahl begrenzen auf maximal n Stück

Bei aktivierter Option kann die maximale Anzahl von Berichten auf eine bestimmte Menge begrenzt werden; erlaubte Werte sind: 1 bis 300. Wird die angegebene Anzahl überschritten, werden die jeweils ältesten Berichte gelöscht.

Alle Berichte löschen älter als n Tag(e)

Bei aktivierter Option werden Berichte nach einer gewissen Anzahl von Tagen automatisch gelöscht; erlaubte Werte sind: 1 bis 90 Tage. Diese Option ist standardmäßig mit einem Wert von 30 Tagen aktiviert.

Keine Begrenzung

Bei aktivierter Option ist die Anzahl der Berichte nicht begrenzt.

12.10.8 Verzeichnisse

Temporärer Pfad

Systemeinstellung verwenden

Bei aktivierter Option werden für die Handhabung von temporären Dateien die Einstellungen des Systems verwendet.

> **Hinweis**
> Wo Ihr System temporäre Dateien speichert finden Sie - am Beispiel von Windows XP - unter: **Start > Einstellungen > Systemsteuerung > System >** Registerkarte "**Erweitert**" > Schaltfläche "**Umgebungsvariablen**". Die temporären Variablen (`TEMP`, `TMP`) für den jeweils angemeldeten Benutzer als auch für Systemvariablen (`TEMP`, `TMP`) sind hier mit ihren entsprechenden Werten ersichtlich.

Folgendes Verzeichnis verwenden

Bei aktivierter Option wird der im Eingabefeld angezeigte Pfad verwendet.

Eingabefeld

In diesem Eingabefeld tragen Sie den Pfad ein, unter dem temporäre Dateien vom Programm abgelegt werden sollen.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, den gewünschten temporären Pfad auszuwählen.

Standard

Die Schaltfläche stellt das vordefinierte Verzeichnis für den temporären Pfad wieder her.

12.10.9 Akustische Warnung

Beim Fund eines Virus oder einer Malware durch den System-Scanner oder den Echtzeit-Scanner ertönt im interaktiven Aktionsmodus ein Warnton. Sie haben die Möglichkeit, den Warnton zu deaktivieren oder zu aktivieren sowie eine alternative WAVE-Datei als Warnton auszuwählen.

> **Hinweis**
> Der Aktionsmodus des System-Scanners wird in der Konfiguration unter PC

Sicherheit > System-Scanner > Suche > Aktion bei Fund eingestellt. Der Aktionsmodus des Echtzeit-Scanners wird in der Konfiguration unter PC Sicherheit > Echtzeit-Scanner > Suche > Aktion bei Fund eingestellt.

Keine Warnung

Bei aktivierter Option erfolgt keine akustische Warnung bei einem Virenfund durch den System-Scanner oder den Echtzeit-Scanner.

Über PC-Lautsprecher abspielen (nur bei interaktivem Modus)

Bei aktivierter Option erfolgt eine akustische Warnung mit dem Standardwarnton beim Fund eines Virus durch den System-Scanner oder den Echtzeit-Scanner. Der Warnton wird über den PC internen Lautsprecher abgespielt.

Folgende WAVE-Datei benutzen (nur bei interaktivem Modus)

Bei aktivierter Option erfolgt bei Fund eines Virus durch den System-Scanner oder den Echtzeit-Scanner ein akustisches Warnen mit der ausgewählten WAVE-Datei. Die ausgewählte WAVE-Datei wird über einen angeschlossenen externen Lautsprecher abgespielt.

WAVE-Datei

In diesem Eingabefeld können Sie den Namen und den dazugehörigen Pfad einer Audiodatei Ihrer Wahl eintragen. Der Standardwarnton des Programms ist als Voreinstellung eingetragen.



Die Schaltfläche öffnet ein Fenster, in dem Sie die Möglichkeit haben, die gewünschte Datei mit Hilfe des Datei-Explorers auszuwählen.

Test

Diese Schaltfläche dient zum Testen der ausgewählten WAVE-Datei.

12.10.10 Warnungen

Ihr Avira Produkt erzeugt bei bestimmten Ereignissen Desktopbenachrichtigungen, sogenannte Slide-Ups, um Sie über Gefahren sowie erfolgreich ausgeführte oder fehlgeschlagene Programmabläufe, wie z.B. die Ausführung eines Updates, zu informieren. Unter **Warnungen** können Sie die Benachrichtigung bei bestimmten Ereignissen aktivieren oder deaktivieren.

Bei Desktop-Benachrichtigungen besteht die Möglichkeit, die Benachrichtigung direkt im Slide-Up zu deaktivieren. Sie können die Deaktivierung der Benachrichtigung im Konfigurationsfenster **Warnungen** rückgängig machen.

Update



Warnung, falls letztes Update älter als n Tag(e) ist

In diesem Feld können Sie die Anzahl an Tagen eingeben, die seit dem letzten Update maximal vergangen sein dürfen. Ist dieser Zeitraum überschritten, wird im Control Center unter Status ein rotes Icon für den Update-Status angezeigt.

Hinweis anzeigen, falls Virendefinitionsdatei veraltet

Bei aktivierter Option erhalten Sie im Fall einer veralteten Virendefinitionsdatei eine Warnmeldung. Mit Hilfe der Option "Warnung, falls letztes Update älter als n Tag(e)" können Sie den zeitlichen Abstand zur Warnmeldung konfigurieren.

Warnungen / Hinweise bei folgenden Situationen

Dial-Up Verbindung wird verwendet

Bei aktivierter Option werden Sie mit einer Desktop-Benachrichtigung gewarnt, wenn auf Ihrem Rechner ein Einwahlprogramm über das Telefon- oder das ISDN-Netz eine Wählverbindung aufbaut. Es besteht die Gefahr, dass es sich bei dem Einwahlprogramm um einen unbekannten und unerwünschten Dialer handelt, der eine kostenpflichtige Verbindung erstellt. (siehe Gefahrenkategorien: Kostenverursachende Einwahlprogramme)

Dateien wurden erfolgreich aktualisiert

Bei aktivierter Option erhalten Sie eine Desktop-Benachrichtigung, wenn ein Update erfolgreich abgeschlossen wurde und Dateien aktualisiert wurden.

Update ist fehlgeschlagen

Bei aktivierter Option erhalten Sie eine Desktop-Benachrichtigung, wenn ein Update fehlgeschlagen ist: Es konnte keine Verbindung zum Downloadserver aufgebaut werden oder die Update-Dateien konnten nicht installiert werden.

Es ist kein Update notwendig

Bei aktivierter Option erhalten Sie eine Desktop-Benachrichtigung, wenn ein Update angestoßen wurde, die Installation von Dateien jedoch nicht erforderlich war, da Ihr Programm auf dem aktuellsten Stand ist.

Ausgabe Q2/2013



live *free.*™

Avira Operations GmbH & Co. KG
Kaplaneiweg 1 | 88069 Tettnang
Germany

Telefon: +49 7542-500 0
Telefax: +49 7542-500 3000
www.avira.de